NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A FRAMEWORK FOR SYNTHESIZING THE UNITED STATES CODE IN SUPPORT OF CYBERSPACE OPERATIONS

by

Joshua C. Stonehouse

March 2016

Thesis Advisor: Dorothy Denning
Second Reader: Wade Huntley

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE A FRAMEWORK FOR SYNTHESIZING THE UNITED STATES CODE IN SUPPORT OF CYBERSPACE OPERATIONS			**5. FUNDING NUMBERS**
6. AUTHOR(S) Joshua C. Stonehouse			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

In recent years, federal agencies and organizations have witnessed their jurisdictions converge in a number of areas that support U.S. national security. For operations that rely heavily upon information technology, the complexity associated with clarifying statutory authority has been met with inconsistent responses. Attempts to comprehend the technological implications of these operations has been accompanied by a shift in seeing the United States Code (U.S.C.) as providing mutually exclusive authorities to government entities operating in cyberspace. While many recognize that cyberspace poses new and unique challenges to inter-title operations, it is unclear whether this de facto shift in the application of U.S.C. statutes is necessary. The U.S.C. has a limited number of exclusionary distinctions *de jure*, which is attested to by a long history of inter-title cooperation that efficiently and effectively supports government operations. Most of the concerns over the United States Code can be appropriately categorized in terms of oversight and compliance requirements, fiscal controls, and statutory responsibilities. This thesis addresses these statutory concerns and culminates with a planning framework that can be used to enable military and other government agencies to support multiple title authorities cooperating seamlessly to effectively plan and execute cyberspace operations.

14. SUBJECT TERMS cyberspace, congressional oversight, title authorities, United States Code, U.S.C., cyberspace operations, inter-title, joint planning, operational planning, cyberspace planner, 6 USC, Title 6, 10 USC, Title 10, 14 USC, Title 14, 18 USC, Title 18, 28 USC, Title 28, 32 USC, Title 32, 50 USC, Title 50, operational framework, inter-title framework, cyberspace framework			**15. NUMBER OF PAGES** 225 / **16. PRICE CODE**
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A FRAMEWORK FOR SYNTHESIZING THE UNITED STATES CODE IN SUPPORT OF CYBERSPACE OPERATIONS

Joshua C. Stonehouse
Lieutenant Commander, United States Navy
B.S., Illinois Institute of Technology, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2016

Approved by: Dorothy Denning
Thesis Advisor

Wade Huntley
Second Reader

Cynthia Irvine
Chair, Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In recent years, federal agencies and organizations have witnessed their jurisdictions converge in a number of areas that support U.S. national security. For operations that rely heavily upon information technology, the complexity associated with clarifying statutory authority has been met with inconsistent responses. Attempts to comprehend the technological implications of these operations has been accompanied by a shift in seeing the United States Code (U.S.C.) as providing mutually exclusive authorities to government entities operating in cyberspace. While many recognize that cyberspace poses new and unique challenges to inter-title operations, it is unclear whether this de facto shift in the application of U.S.C. statutes is necessary. The U.S.C. has a limited number of exclusionary distinctions de jure, which is attested to by a long history of inter-title cooperation that efficiently and effectively supports government operations. Most of the concerns over the United States Code can be appropriately categorized in terms of oversight and compliance requirements, fiscal controls, and statutory responsibilities. This thesis addresses these statutory concerns and culminates with a planning framework that can be used to enable military and other government agencies to support multiple title authorities cooperating seamlessly to effectively plan and execute cyberspace operations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS, ABBREVIATIONS, AND TERMS

AFA	Air Force Association
AFTTP	Air Force Tactics, Techniques, and Procedures
ALSA	Air Land Sea Application Center
APT	Advanced Persistent Threat
ATP	Army Techniques Publication
AUMF	Authorization for Use of Military Force
BENS	Business Executives for National Security
CAA	Consolidated Appropriations Act
CCDCOE	Cooperative Cyber Defence Center of Excellence
CCIPS	Computer Crime and Intellectual Property Section
CFAA	Computer Fraud and Abuse Act
CGCYBERCOM	Coast Guard's Cyber Command
CHS	House Committee on Homeland Security
CIA	Central Intelligence Agency
CIKR	Critical Infrastructure and Key Resources
CIP	Critical Infrastructure Protection
CISA	Cybersecurity Information Sharing Act
CMF	Cyber Mission Forces
CMT	Combat Mission Team
CNE	Computer Network Exploitation
COCOM	Combatant Commander
CPU	Central processing unit
CPT	Cyber Protection Team
CRS	Congressional Research Service
CS&T	Senate Commerce, Science, and Transportation Committee
CSIS	Center for Strategic and International Studies
CSS	Central Security Service
DCO-RA	Defensive Cyber Operations, Response Actions
DDI	Directorate for Digital Innovation
DDOS	Distributed denial of service
DHS	Department of Homeland Security
DIOG	Domestic Investigations and Operations Guide
DNI	Director of National Intelligence
DOD	United States Department of Defense
DOJ	United States Department of Justice
DOS	Denial of Service
DOS	United States Department of State
DOT	United States Department of Transportation
DSC	Dual Status Commander

DSCA	Defense Support of Civil Authorities
DTR	Defense Transportation Regulation
ECPA	Electronic Communications Privacy Act
EDT	Electronic Disobedience Theater
EMAC	Emergency Management Assistance Compact
EO	Executive Order
F.R.	Federal Record
FAA	FISA Amendments Act
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FISA	Foreign Intelligence Surveillance Act
FISC	United States Foreign Intelligence Surveillance Court
FOIA	Freedom of Information Act
H.R.	House Resolution
H. Doc.	House Document
H. Rep.	House Report
HASC	House Armed Services Committee
HFN	Hastily Formed Networks
HJC	House Judiciary Committee
HPSCI	Permanent Select Committee on Intelligence of the House of Representatives
HSGAC	Senate Committee on Homeland Security and Governmental Affairs
HSIN-CI	Homeland Security Information Network for Critical Infrastructure
IC	Intelligence Community
IC3	Internet Crime Complaint Center
ICC	International Criminal Court
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IO	Information Operations
IRTPA	Intelligence Reform and Terrorism Prevention Act
IT	Information Technology
ITU	International Telecommunication Union
JMEM	Joint Munitions Effectiveness Manual
JOC	Joint Operations Center
JOPP	Joint Operational Planning Process
JP	Joint Publication
JIPTL	Joint Integrated Prioritized Target List
JTF	Joint Task Force

JTF-Katrina	Joint Task Force Katrina
JTF-LA	Joint Task Force Los Angeles
LFA	Lead Federal Agency
M/V	Motor Vessel
MCWP	Marine Corps Warfighting Publication
MOA	Memorandum of Agreement
NATO	North Atlantic Treaty Organization
NCC	National Coordinating Center for Communications
NCCIC	National Cybersecurity and Communications Integration Center
NCIRP	National Cyber Incident Response Plan
NCPC	National Counter Proliferation Center
NCPS	National Cybersecurity Protection System
NCTC	National Counterterrorism Center
NDAA	National Defense Authorization Act
NIC	National Intelligence Centers
NMT	National Mission Team
NO&I	NCCIC Operations & Integration
NRF	National Response Framework
NS/EP	National Security or Emergency Preparedness
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSC	National Security Council
NSD	National Security Division
NSL	National Security Letters
NTTP	Navy Tactics, Techniques, and Procedures
OCO	Offensive Cyber Operations
OCTF	Organized Crime Task Force
ODNI	Office of the Director of National Intelligence
OLH	Operational Law Handbook
OPE	Operational Preparation of The Environment
PAA	Protect America Act
PCA	Posse Comitatus Act
PDA	Preliminary Damage Assessment
PG&E	Pacific Gas and Electric Company
PLA	People's Liberation Army
PPD	Presidential Policy Directive
PSCP	Private Sector Clearance Program for Critical Infrastructure
PTSN	Public Switched Telephone Network

RICO	Racketeer Influenced and Corrupt Organizations
ROE	Rules of Engagement
S.	Senate Bill
S. Doc.	Senate Document
S. Rep.	Senate Report
S/CCI	State Department's Office of the Coordinator for Cyber Issues
SAD	State Active Duty
SARS	Severe Acute Respiratory Syndrome
SASC	Senate Armed Services Committee
SCA	Stored Communications Act
SIGINT	Signals Intelligence
SJC	Senate Judiciary Committee
SLLE	State and Local Law Enforcement
SSA	Sector Specific Agency
SSCI	Senate Select Committee on Intelligence
T&I	House Transportation and Infrastructure Committee
TAO	Tailored Access Operations
TCC	Tactical Coordination Center
TCO	Transnational Criminal Organization
TIARA	Tactical Intelligence and Related Activities
Treasury	United States Department of the Treasury
U.S.C. (also USC)[1]	United States Code
UCMJ	Uniform Code of Military Justice
US-CERT	United States Computer Emergency Readiness Team
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
USA FREEDOM	Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act
USCG	United States Coast Guard
USCYBERCOM	United States Cyber Command
USNORTHCOM	United States Northern Command
USSOUTHCOM	United States Southern Command
VoIP	Voice over IP

[1] In cases where specific title codes are referenced within the United States Code, 10 USC is synonymous with Title 10. The former is more likely to be used when it is accompanied by a specific section (i.e. 10 USC § 3001).

ACKNOWLEDGMENTS

I would like to thank Dr. Dorothy Denning for her encouragement and advice on the content and direction of this thesis. Her course on Conflict and Cyberspace inspired me to contribute to the ongoing conversation on the government's role in cyberspace, which is by no means nearing completion. Dr. Denning's professional body of work is an inspiration, and her sharp clarity provided the expertise needed to finish out my postgraduate coursework with this culminating piece.

I would also like to thank my second reader, Dr. Wade Huntley, for his feedback and assistance. He consistently challenged me to focus the scope of my examination and to ask whether my conclusions were answering questions that really matter—no small task, I might add.

I would like to thank my beautiful family who provided me with constant encouragement and the time to pursue my studies and writing. My father, in particular, spent countless hours poring over drafts and providing invaluable feedback, and my wife and children constantly reinvigorated me with their contagious exuberance that held up, even under long absences. Thank you.

Lastly, I feel a debt of gratitude to the many contributors whose clarity in understanding the law made this difficult task significantly easier. Andru Wall and Robert Chesney had inspired me long before I undertook this endeavor, and I am thankful for their keen insights and pragmatic approaches. They have profoundly changed the way I perceive operations—of which the military is just a piece of the greater whole.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OBJECTIVE

As a rule, operational planners do not have the luxury of time to identify inefficiencies, uncover the source of apparent policy contradictions, or innovate methods for mission planning. Rather, their taxing workload forces them to seek the path of least resistance, which frequently prioritizes clarity over correctness and acceptability over opportunity. Operational planners find themselves burdened with the imminency of conflict and a labyrinth of domestic and international legislation that can be paradoxically both coherent and confusing.[1] In this environment, taking the time to ask the right questions and to discover and follow relevant lines of inquiry are likely to result in missed deadlines and may fail to generate admiration from superiors. This is not a criticism but a depiction of the dilemma that faces the majority of planners because, at some point, the time for questions and reexaminations must end and deliverables must be created. In the rapidly expanding field of cyberspace, cyber planners have more red tape,[2]

[1] *See* generally CYBERSPACE OPERATIONS. International and Operational Law Department, "Operational Law Handbook," David H. Lee, ed. (The Judge Advocate General's Legal Center and School, U.S. Army, 2015): 145–50, https://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdf. The Operational Law Handbook (OLH) states that although "no international treaty or domestic statute comprehensively governs U.S. military activities in cyberspace, a number of policy and regulatory documents—both classified and unclassified—provide guidance to legal advisors on applying existing laws to [Cyber Operations (CO)]." *See* also Carlos Jose Gutierrez, "Conflicts Between Domestic and International Law," *The American University Law Review* 30, no. 1 (Fall 1980): 153. When "we are not dealing with isolated acts, but rather, with systematic policies maintained by governments, we no longer can speak in terms of simple violations but must recognize a real conflict between the domestic legal order and the international instrument that establishes duties that the state does not intend to fulfill." *See* also Michael J. Glennon, *The Fog of Law* (Washington D.C.: Woodrow Wilson Center Press, 2010), 81–84. In the international and domestic legal systems, there are significant differences in the ways and means by which laws are created, enacted, and repealed. In the domestic system, "laws are made by legislators or […] someone other than the person on the street. The actions of a bank robber therefore do not affect the validity of the law that prohibits bank robbery. In the international system, however, states are the participants and lawmakers, and "their actions have direct juridical effects. Repeated state actions that are at odds with an existing customary rule have the effect of modifying or eliminating the rule" altogether.

[2] *See* FULL DEFINITION OF RED TAPE. *Merriam Webster Online Dictionary*, s.v. "red tape," accessed January 13, 2016, http://www.merriam-webster.com/dictionary/red%20tape. Merriam-Webster defines red tape as "official routine or procedure marked by excessive complexity which results in delay or inaction."

less clarity,[3] and higher expectations[4] than almost any other kind of planner. It is within this paradigm that this thesis seeks to expose possibilities and provide conclusive options for planners—cyber planners in particular—which they might otherwise not have the time to ponder or pursue.

Stated simply, the objective of this thesis is to develop a framework that addresses the statutory authorities contained in the United States Code. It incorporates the corresponding oversight and compliance requirements, as well as fiscal controls in a way that will enable military and other government agencies to utilize it to support multiple title authorities working cooperatively and seamlessly to effectively plan and execute cyberspace operations. This is no easy task, as the sheer volume of legislation, continual fluctuations in legal opinion, and modifications to law and legal implementation threaten to contradict or make obsolete the conclusions of this work before the ink is dry, as it were.

B. RESEARCH QUESTIONS

Amid these endeavors, a fundamental question is this: How can the government enable integrated cyberspace operations? Answering this is difficult enough when restricting factors and considerations to the armed forces[5] alone, but it can develop into an unmanageable task when attempting to fold in the myriad of additional state and federal actors who are already operating in

[3] *See* generally, Mark A. Gallagher and Michael Horta, "Cyber Joint Munitions Effectiveness Manual (JMEM)," *M&S Journal* (Summer 2013): 5–14. Though not conclusive, one example of the disjointed nature of cyber planning is the lack of a Joint Munitions Effectiveness Manual (JMEM) for cyber, the absence of which makes it extremely difficult to assess the effects of using cyber munitions during and leading up to hostilities. More than that, it is almost impossible for Unified Combatant Commanders in the Department of Defense (DOD) to fold Offensive Cyber Operations (OCO) into a Joint Integrated Prioritized Target List (JIPTL).

[4] Among many notable cyber-influenced changes to law as well as state and federal organizational structures, the last decade has seen over 350 instances of the word, "cyber" being added to the U.S. Code, the DOD's release of Joint Publication 3-12 (Cyberspace Operations), and the signing into law of the Cybersecurity Information Sharing Act (CISA) on December 18, 2015. This increase in requirements has hardly been complimented by consensus on the nature of cyber conflicts, the creation of uniform cyber planning models, or even a shared cyber lexicon.

[5] Those services created under U.S. Code, 10 USC §§ 3001,5001,8001 to include relevant sections governing the employment of the Coast Guard subject to 10 USC § 5013a and 14 USC § 3.

cyberspace. This is because the previous question is not merely concerned with breaking down cultural barriers in order to enable one agency to extend an olive branch to another. As such, a more substantive question is this:

> What allowances are available and what concerns must be addressed to allow U.S. federal and state governments to include subordinate militaries and agencies in conducting integrated planning and execution of cyberspace operations?

In order to answer this question, however, many secondary questions require answers, as well.

1. Is there a legal precedent for mutually supportive operational interaction between U.S.C. title authorities?
2. What are the advantages and disadvantages of operating under multiple U.S.C. title authorities?
3. What (if any) legal restrictions exist that govern or limit action of U.S.C. title authorities operating in cyberspace?
4. What are the oversight and compliance requirements, and fiscal controls that govern each of the U.S.C. title authorities?
5. Where should authorities be delegated for approving and disapproving cyberspace plans and operations?
6. What changes (if any) must be made to the U.S.C. in order to enable cyberspace operations?

This thesis will consolidate relevant conclusions and much of the work that has been invested into answering these questions and the previously stated primary question. Many of the ensuing discussions will focus on providing an overarching context from which the final framework will emerge.

C. DISCUSSION

To frame the pursuit of answers to these critical questions, it is important to acknowledge the many agencies and military organizations with active U.S. charters to operate in cyberspace. These groups continue to be levied with growing expectations and compounding restrictions that are doled out by a host of governing authorities through disparate systems of dissemination. Some of

this is simply organizational policy while other demands become binding through public law. In either case, they tend to be linked to a swell of oversight and compliance measures imposed by the Executive, Legislative, and Judicial branches of the federal government. Tensions between these branches along with recent and dramatic shifts in public trust have put the United States Code front and center in a debate that is greatly focused on assuaging political pressures rather than addressing pragmatic concerns.

This debate is nowhere more heated than the often referred to "Title-10/Title-50" debate[6] but has more recently grown to include Title 6 (Homeland Defense), Title 14 (Coast Guard), Title 18 (Crimes and Criminal Procedure), Title 28 (Judiciary and Judicial Procedure), and Title 32 (National Guard). Although there are organizations operating in cyberspace under additional U.S. Codes,[7] these receive the majority of scrutiny due to their frequently overlapping agendas, perceived public impact, and similarities in operational procedure. As a result, there is disagreement as to what constitutes appropriate interactions within and between these entities as they operate under distinct title authorities and sections within the United States Code. Members of agencies and organizations operating in cyberspace may reach out to one another under an approved memorandum of agreement (MOA). They may also coordinate efforts under the information sharing mandates that came as a result of recommendations from the 9/11 Commission.[8] However, without an agreed upon framework and in the absence of tacit approval, they do so at their own peril.

---

[6] Title 10 (Armed Forces) outlines the role of the military. Title 50 (War and National Defense) is significantly more diverse. It not only governs espionage and makes provision for intelligence agencies (e.g., CIA and NSA), but it also outlines authorities for and governs instances of insurrection and national emergency among others.

[7] Most notably, Title 15 (Commerce and Trade) and Title 42 (The Public Health and Welfare) of the U.S.C. have numerous stipulations related to responsibilities for managing and responding to cybersecurity requirements and cyber-threats. The majority of actors, however, are covered under the U.S.C. Title authorities addressed here.

[8] *See* generally "Information Sharing," U.S. Department of Homeland Security, last modified August 26, 2015, http://www.dhs.gov/topic/information-sharing.

Many critics remark that current methods for planning and execution are not possible within the paradigm shift presented by cyberspace. One of the major sources of this tension derives from the highly technical and oft-misunderstood nature of cyberspace.[9] Its composition of both logical and physical components presents complications to executing operations that are seen by some critics as insurmountable under the current legal framework.[10] It is important to note here that inter-title cooperation is not, nor should it be interpreted as, an attempt to circumvent international law. In many countries, the security forces responsible for enforcing domestic law are nearly indistinguishable from those responsible for subduing international conflicts. The United States has a long history of separating international forces from domestic ones, but regardless of force composition, inter-title cooperation is about effectiveness and efficiency, and not intended to alleviate the weight of legal responsibility.

Certainly, there are unique challenges posed by the cyberspace domain, for which new legislation could bring some clarity, but an overhaul of the United States Code and inter-title interactions is likely unnecessary. The National Security Strategies produced by both the George W. Bush administration (2002, 2006) and the Barak Obama administration (2010, 2015) placed heavy emphasis on the need for government agencies—not exclusively the military—to disrupt and neutralize terrorist networks. Even just a small sample of the well-documented use of cyberspace by terrorist networks[11] can lead to reasonable

---

[9] *See* generally Martha S. H. VanDriel, "Bridging the Planning Gap: Incorporating Cyberspace Into Operational Planning," *Strategic Studies Institute, U.S. Army War College*, May 4, 2015, http://www.strategicstudiesinstitute.army.mil/index.cfm/articles/Bridging-the-planning-gap/2015/05/04. VanDriel enumerates numerous obstacles to cyberspace planning. Widespread ignorance on capabilities, command, and planning structures lead to unsuccessful attempts to incorporate cyberspace into overall operational planning.

[10] Michael J. Glennon, "The Road Ahead: Gaps, Leaks and Drips," *International Law Studies* 89, (2013): 367–69. While Glennon correctly exposes the incompleteness of international law in addressing cyber conflict, the current legal frameworks may still support inter-title cooperation.

[11] *See* generally Stuart Macdonald and David Mair, "Terrorism Online: A New Strategic Environment," in *Terrorism Online: Politics, Law and Technology*, eds. Lee Jarvis, Stuart Macdonald, and Thomas M. Chen, (New York: Routledge, 2015), 10–24. Macdonald and Mair broadly enumerate terrorist groups' use cyberspace to conduct outreach, enable logistics, and conduct physical, psychological, and cyber-based attacks.

conclusions about how multiple title authorities are likely to be operating in cyberspace in similar and mutually supportive ways to achieve these national security objectives.

D. BENEFITS

As cyberspace becomes more pervasive, adversaries of the United States will continue to leverage its power to undermine national security. As such, it is imperative that a framework be developed for understanding how to best enable cooperation and synthesize cyberspace operations between the many organizations operating under various title authorities. Developing this framework can not only effect planning and operations but also lead to greater fiscal efficiency. A recurring theme in cyberspace discussions is the need for a robust information technology (IT) infrastructure that is capable of providing for national security and advancing national interests. In an era where budgetary constraints and austerity measures are becoming increasingly more common, a framework that allows for greater coordination and enables diffused resources to be focused toward a common goal should lead to increased sustainment in supporting broad-spectrum cyberspace operations.

E. THESIS OUTLINE

To address these challenges and concerns in a coherent way, this thesis is divided into six chapters. This chapter provides the introductory material to the thesis, its objectives, benefits, methodologies, and the scope of the study.

As alluded to earlier, one of the major challenges with this subject is the belief that there is something unethical or even illegal about coopting two or more title-authorities into the same operation. Therefore, the second chapter provides a summary of concerns over the United States Code. It explores the lengthy discourse that has accompanied interpretations and employment of the United States Code throughout its history. This chapter also makes initial progress in isolating significant elements of the proposed framework by identifying relevant authorities, agencies, and organizations within the U.S. Code. It further

addresses the perceptions and controversies in the context of relevant legislation.

Based on the findings outlined in the second chapter, the third chapter outlines applicable statutes for enabling inter-title operations. Discussions in this chapter focus on historical examples and ongoing operations that are primarily characterized by inter-title support. Conclusions will contextualize statutory authorities to either enable or preclude aspects of inter-title cooperation amidst the unique dilemmas presented by the cyberspace domain.

The fourth chapter presents the culmination of previous work by outlining statutory requirements and suggesting a framework that will enable planners to appropriately understand the requirements, constraints, and opportunities for inter-title interactions as they are supported by the United States Code.

The fifth chapter utilizes this framework to present two scenarios for possible inter-title cooperation. The first scenario, “Inter-Title Cyberspace Support to Counterproliferation Operations,” explores oversight and compliance, and fiscal concerns related to inter-title cooperation in a counterproliferation environment. This scenario explores authorities governed primarily by 10 USC, 14 USC, 18 USC, and 50 USC. The second scenario, “Inter-Title Cyberspace Support to Defense of Critical Infrastructure,” explores possibilities for enabling cooperation in the defense of critical infrastructure under 6 USC, 10 USC, 32 USC, and 50 USC. These types of interactions are neither new nor innovative. In many cases, they are simply not understood by those who participate in them. The framework and the scenarios, therefore, are simply designed to make explicit for policy makers, operational planners, and even legislators what has already been made possible by law.

The sixth chapter is concerned with the findings and recommendations for future work. This chapter consolidates conclusions drawn from the research and provides a summary of the most essential elements of the thesis and its suggested framework. It addresses some of the perceived dilemmas created by

applying the U.S.C. to the cyberspace domain, and exposes the benefits of inter-title cooperation as well as possible costs associated with gaining greater efficiencies. Additionally, it highlights issues that are beyond the scope of this thesis but in need of further research.

II. CURRENT AND HISTORICAL CONCERNS OVER THE UNITED STATES CODE

A. EIGHTY YEARS OF WAR AND THE NATION STATE

Though statecraft has progressed through numerous iterations over the course of human history, in the current post-colonial era, the success[12] of the nation state is largely linked to its sovereign ability to establish and exercise law within its territorial borders.[13] The failure of fascism—made permanent by the decisive conclusion to WWII--and the near-extinction of communism by the turn of the 21st century[14] led to the broad establishment of parliamentarian rule—most commonly referred to as democracy—as the most prolific form of state governance.[15,] World Wars I and II, the Korean War, the Vietnam War, and even the Soviet-Afghan War were arguably most significantly influenced by competing identities of nation-state governance. With the resolution of these and other conflicts of the Cold-War era,[16] the world has seen democratic rule firmly established as the most popular form of governance. This development is

---

[12] *See* generally "Indicators," Fund for Peace, accessed September 25, 2015, http://fsi.fundforpeace.org/indicators. The *Fund for Peace* is an independent research organization that defines 12 indicators of state stability. While they fall into the three general categories of Social, Economic, and Political-Military, they are all highly dependent on a robust and equitable legal framework from which the nation can provide reliable governance and security.

[13] Philip Bobbitt, *The Shield of Achilles: War, Peace, and the Course of History* (New York: Anchor Books, 2003), xxii.

[14] Archie Brown, *The Rise and Fall of Communism* (London: The Bodley Head, 2009), 606. As of 2009, only five nations claimed a form of Communist governance and Brown asserts that most influential of these—China—had discarded enough of its Communist indicators by 2000 to be, at best, a hybridized socialist government.

[15] *See* generally Max Roser, "Democratisation," Our World in Data, accessed November 4, 2015, http://ourworldindata.org/data/political-regimes/democratisation. Max Roser, an Oxford University researcher, estimates that in 2015, approximately 70% of the world population lived in countries with a significant degree of democratization. *See* also Economist Intelligence Unit, "Democracy Index 2014," *Economist*, accessed November 4, 2015, available through http://www.eiu.com/democracy2014. Report indicates that in 2014, over 60% of all countries had implemented significant democratic processes for its citizens.

[16] *See* generally *Wikipedia*, s.v. "Cold War," last modified March 8, 2016, https://en.wikipedia.org/wiki/Cold_War. Circa 1947–1991 is a generally agreed-upon timeframe for the Cold War.

significant because, while parliamentarian rule has emerged as the most dominant form of the nation state, its advantages are accompanied by unique susceptibilities to global threats that exist within and yet extend beyond each nation's borders. Although conflicts and threats to rule have admittedly traversed regional boundaries for thousands of years, the global threats that have emerged from the conflict of the 20th century stand out as unique, not only in their sheer breadth but also in how they are perceived by the nation state. They are distinctive from past threats in that they are common to each nation yet beyond the capacity of any to individually address on its own. While nearly 80 years of war[17] saw many course changes for the nation state to reach its final and nominally unchallenged status, this time period had also ushered in a new era of unique vulnerabilities and challenges that currently threaten to destabilize parliamentarian rule as a governmental hegemon.

To begin with, the conflicts of the 20th century gave rise to global organizations like the United Nations[18] and North Atlantic Treaty Organization,[19] which instituted international mandates on human rights[20] and a system for international law,[21] and which developed increasingly pejorative views on

[17] The 77-year period of conflict from 1914 (start of WWI) to 1991 (ending in the dissolution of the Soviet Union).

[18] *See* generally "History of the United Nations," United Nations, accessed December 10, 2015, http://www.un.org/en/sections/history/history-united-nations. *See* also United Nations, *Charter of The United Nations*, October 24, 1945, Ch. I, Art. 1, accessed December 10, 2015, http://www.un.org/en/ sections/un-charter/chapter-i/index.html. The United Nations was formed amidst the conflict of WWII in order to combat the axis powers and with the expressed purpose "to take effective collective measures for the prevention and removal of threats to the peace".

[19] *See* generally North Atlantic Treaty Organization, "A Short History of NATO," accessed December 10, 2015, http://www.nato.int/history/nato-history.html. The creation of NATO was founded in "deterring Soviet expansionism, forbidding the revival of nationalist militarism in Europe through a strong North American presence on the continent, and encouraging European political integration."

[20] *See* generally United Nations, General Assembly, *International Bill of Human Rights,* December 10, 1948, A/RES/217(III), accessed November 8, 2015, http://www.undocs.org/A/RES/217(III).

[21] *See* generally Glennon, *The Fog of Law*, 30–36. International Law has seen a great deal of controversy since its outset. Its effectiveness and legitimacy have been called into question by disagreement over the permanency of *consent* given by its participants, its dependency on states to impose the *obligation* of law upon themselves, and the complex motives that govern states' participation which occlude identifying a standard *c*ausation for constituting a norm.

unilateral action of nation states acting in their own self-interest.[22] In addition, the development of global trade networks has created new and powerful efficiencies in the manufacturing and commodities markets,[23] but, in the absence of global consensus between nations, has also created labor and manufacturing dependencies that have remained largely under auspices of international companies and corporations to manage. The expansion of international travel and trade has resulted in softer borders, increased human migration, and increased global exposure to a multitude of communicable diseases like cholera, HIV/AIDS, Severe Acute Respiratory Syndrome (SARS), and influenza.[24] Increased awareness of global ecological dependencies and the transnational effects of industrial pollution, famine, and overfishing have placed many countries at the center of international criticism and contributed to growing tensions between economic allies and competitors alike.[25] Lastly, and probably most significantly, is the creation of global communications networks—of which the Internet[26] is likely the most prominent. These networks have enabled the communication of ideas and information at near-instantaneous speeds, which has led to rapid and effective coordination between previously inaccessible or disparate parties. Despite the obvious benefits of network communications for supporting and advancing national interests, they are being increasingly leveraged to consolidate the interests of transnational populations within, across,

---

[22] *See* INTRODUCTION. Diane F. Orentilicher, "Unilateral Multilateralism: United States Policy Toward the International Criminal Court," *Cornell International Law Journal* 36, no. 3, Article 1 (2004): 415–17, http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1526&context=cilj. While the United States has long advocated for increased multilateral action, their commitment historically favors unilateral action when multilateral authority threatens to exercise jurisdiction over U.S. citizens and U.S. interests.

[23] Thomas L. Friedman, *The World is Flat 3.0: A Brief History of the 21st Century* (New York: Picador, 2007), 573.

[24] *See* generally Andrew J. Tatem, Simon I. Hays, and David J. Rogers, "Global Traffic and Disease Vector Dispersal," *Advances in Parasitology* 62 (April 18, 2006): 6242–47, doi:10.1073/pnas.0508391103.

[25] *See* generally Manfred B. Steger, *Globalization: A Very Short Introduction* (Oxford: Oxford University Press, 2013) 91–95.

[26] *See* generally *Wikipedia*, s.v. "Internet," last modified March 8, 2016, https://en.wikipedia.org/wiki/Internet.

and beyond national borders. These transnational constituencies are able to operate with an agility and agenda that often undermines a nation's interests and even its national security. For the purposes of this thesis, this latter subject is the primary concern, namely cyberspace,[27] though, for at least two major reasons, the former observations are by no means irrelevant.

First, since most of the ensuing discussions are concerned with questions of a legal and ethical nature, it is important to understand the statutory legacy within the historical context that has produced the current *corpus juris*. A pragmatic approach[28] to cyberspace operations demands that these laws—no less the approaches to implementing and enforcing them—should be freshly examined, as nations progress in their understanding and use of information technology. This is by no means a new concept. Prior to the outbreak of WWII, gangs in the United States were becoming a major threat to law enforcement. Based on the increasingly violent nature of criminal activity, it became clear that members of these gangs were exercising their Second Amendment right in ways that served to destabilize state and municipal governments instead of in protection of them.[29] The result, and the first of many to follow, was the National Firearms Act of 1934. This example does not lead to a conclusion that the rule of law becomes irrelevant as soon as societal perspectives shift but suggests

[27] *See* generally Chairman, U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12 (R) (Washington DC: CJCS, February 5, 2013): v. Cyberspace is defined by Department of Defense Joint Doctrine as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

[28] *See* generally Glennon, *The Fog of Law*, 1–22. A pragmatic approach to Law is not strictly governed by practical and common sense concerns. It most patently differs from the idealistic approach—among others—in that it is primarily focused on the real-world consequences of ideas that lead to the creation and implementation of laws.

[29] *See* generally Clayton E. Cramer, *For the Defense of Themselves and the State: The Original Intent and Judicial Interpretation of the Right to Keep and Bear Arms* (Westport, CT: Praeger, 1994) 59–73. *C.f.* with *Bliss v. Commonwealth of Kentucky* in *2 Littell 90, 13 Am. Dec. 251* (1822). One of the earliest interpretations of the Second Amendment came in 1822 when the Kentucky Supreme Court ruled that the federal intent of the constitutional amendment (as ratified in the Commonwealth of Kentucky's constitution) was "the right to bear arms in defense of themselves and the state." The interpretation concerning the *common defense* of the state was ratified in the Constitutions of 18 different states by 1845 (15 of those states included clauses for individual ownership rights).

instead that legislation necessarily leads to systems of de facto policy and procedure—like the concealment or unchecked purchasing of firearms—that many, whether through simple repetition or unawareness, believe to be *de jure*. It is the former that should be summarily scrutinized while the latter more often clarified.[30]

The second major reason is owed to the social context in which these discussions are taking place. Many who experienced the fallout from the 9/11 attacks will remember that cyberspace was not perceived to have played a pivotal role in enabling the physical attacks that took place, though it was certainly recognized as a key asset in identifying, tracking, and apprehending those responsible. In the years following 9/11, however, fewer and fewer terrorist attacks have taken place without a cyber element.[31] These are important points for a number of reasons. First, it shows that holistic perspectives on cyberspace are relatively new and so, it should come as no surprise that legislation and its accompanying policy are likely to lag behind not only the threat but also societal perspectives. Second, it rejects the notion that cyberspace has somehow given rise to terrorist networks or transnational criminal organizations (TCO) or that it is the only medium in which they can effectively employ their power to undermine

[30] In some cases, major societal shifts demand a complete reexamination of *de facto* and *de jure* practices. Jim Crow laws of "The South" were subject to such scrutiny during the American Civil Rights Movement. *See* generally, *Wikipedia*, s.v. "Jim Crow laws," last modified March 6, 2016, https://en.wikipedia.org/wiki/Jim_Crow_laws. The Jim Crow laws of the 19th century are an example of racial *de facto* practices of antebellum America becoming *de jure* following the conclusion of the Civil War. It does not take imagination to comprehend that federal and state legislators will often write *de facto* practices into law in response to challenges against their authority.

[31] *See* generally Lorraine Bowman-Grieve, "Cyberterrorism and Moral Panics: A Reflection On the Discourse of Cyberterrorism," in *Terrorism Online: Politics, Law and Technology*, eds. Lee Jarvis, Stuart Macdonald, and Thomas M. Chen, (New York: Routledge, 2015), 86–87.

national security.[32] Even under a preponderance that suggests effectiveness for these transnational networks that predates global communications networks, it is still difficult to deny that cyberspace has provided an unprecedented increase to their capability. The migration of processes to networked architecture has enabled TCOs, terrorists, and even nation states to stabilize and advance organizational goals that, at best, would have been only nominally effective in the years predating the proliferation of networks and information technology.[33]

As nation states, criminal organizations, and even corporations seek to maximize their equities in global markets, they can hardly do so without the use of cyberspace. Many of these entities are operating in cyberspace in positive ways that lead to improved innovation, increased access, and stability. Others, however, seek to build and leverage transnational networks through cyberspace with destructive inclinations that are criminal in nature.[34] It is addressing these latter groups that is the primary concern of this thesis. Among the malicious entities operating in cyberspace, two of the most recognizable are international terrorist networks like Al Qaeda and the Islamic State, and transnational criminal organizations like the Russian organized crime syndicates or the Mexican drug cartels. Hacker groups, sometimes referred to as hacktivists, while just as recognizable as TCOs and terrorists, tend to operate within a limited scope and

[32] *See* generally "Timeline," National Counterterrorism Center, accessed January 10, 2016, http://www.nctc.gov/site/timeline.html. Some examples of terrorist activities carried out without the assistance of cyberspace include, among others: Washington DC, March 9, 1977, a Hanafi Muslim group took control of three buildings and over 150 hostages. Lebanon, April 18 and October 23, 1983, a car bomb exploded outside the U.S. embassy and Marine barracks, respectively. Casualties totaled more than 350 killed or wounded. *See* also "Methods & Tactics," *id.*, accessed January 10, 2016, http://www.nctc.gov/site/methods.html#sarin. Sixteen deaths in the United States over the years spanning 1972–1990 are classified as "terrorist-associated assassination incidents."

[33] *See* CONCLUSION. Macdonald and Mair, "Terrorism Online: A New Strategic Environment," 28. "The terrorists of today may not be new in terms of their organisational structure, but… the Internet has given them far greater reach than ever before."

[34] *See* generally Pew Research, "Cyber Attacks Likely to Increase," October 29, 2014, http://www.pewinternet.org/files/2014/10/PI_FutureofCyberattacks_102914_pdf.pdf.

duration[35] unless they are being coopted by these criminal organizations or possibly a nation state.[36] A rise in independent cyber-criminal organizations that are detached from traditional TCOs,[37] accompanied by an increase in covert action by nation states[38] makes a simple characterization of cyberspace actors nearly impossible. As such, and for the purposes of simplification, when examples are necessary for inter-title discussions, they will primarily be drawn from organizations and situations that are common and shared—even among diverse audiences. It is also worth noting that even though international constituencies like global corporations and human rights groups can profoundly affect the interests of a nation, they are mostly viewed as a positive expression of democratic rule and are not deemed appropriate targets, especially of U.S. cyberspace operations.

---

[35] *See* DEFINING HACKTIVISM AND ANONYMOUS'S [*sic*] PLACE WITHIN THE MOVEMENT. Brian B. Kelly, "Investing in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' Can and Should Influence Cybersecurity Reform," *Boston University Law Review* 92, no. 5 (March 2012): 1663–82, http://www.bu.edu/law/journals-archive/bulr/volume92n4/documents/kelly.pdf. Hacktivist group, *Anonymous*, is often presented as a significant exception to this statement. Their place within the "hacktivist movement," however, is questionable since their "penchant for disaggregation has given way to what some investigators believe is a coherent structure with ad hoc leaders who delegate tasks, select targets, and reprimand disobedient members." This organizational structure, sustained political objectives, and threats to target U.S. infrastructure may place them in a category where they have more in common with cyberterrorism and TCOs than with protestors and political activists.

[36] *See* OPENING STATEMENT by Dana Rohrabacher. U.S. Congress, House, Committee On Foreign Affairs, *Cyber Attacks: An Unprecedented Threat to U.S. National Security: Hearing Before the Subcommittee On Europe, Eurasia, And Emerging Threats of the Committee On Foreign Affairs*, 113th Cong., 1st sess., 2013, 3–4, http://docs.house.gov/meetings/FA/FA14/20130321/100547/HHRG-113-FA14-20130321-SD002.pdf. Specifically, there is no clear international consensus on how to identify, classify, and respond to individual hackers and groups who are being used as proxy forces by various nation states. Adding to this dilemma is the difficulty associated with attribution. *See* also Mandiant Intelligence Center, "APT1: Exposing One of China's Cyber Espionage Units," *Mandiant Corporation* (2013) http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[37] *See* generally Megan Penn, "Organized Cyber Crime: Comparison of Criminal Groups in Cyberspace," *Cyber Defense Review, Policy & Law Blog,* April 7, 2015, http://www.cyberdefensereview.org/2015/04/07/organized-cyber-crime.

[38] *See* COMPUTER NETWORK ATTACK. Walter Gary Sharp, Sr., *CyberSpace and the Use of Force* (Falls Church, VA: Aegis Research Corporation, 1999), 132–33. "Just as with computer espionage, the difficulty in responding to a computer network attack in self defense is determining the identity of the attacking state."

Another factor that receives significantly less attention amid the cloak-and-dagger activities of cyberspace, is the place of inter-title cyberspace operations in support of relief efforts for emergencies and national disasters. The 21st century has introduced the idea of Hastily Formed Networks (HFN) in response to the enormous advantage of networks and the growing societal dependencies upon them.[39] Coordination of relief efforts like food distribution or the reconstitution of banking or ATMs is often as essential as power restoration during long term or widespread emergencies. Federal agencies already provide network infrastructure for services like banking.[40] It is therefore not a significant leap to imagine federal relief workers rapidly constituting ad hoc networks to ensure the restoration of critical sectors. This is an important consideration for inter-title operations and represents an important conversation that must recognize appropriate distinctions between both federal and state jurisdictions.

For all the complex factors that go into the analysis, the simple fact remains that if the United States intends to establish itself equitably within cyberspace, it must do so in a way that legally combats threats that do not tend to operate within the boundaries of domestic and international law.

---

[39] *See* generally Peter J. Denning, "Hastily Formed Networks," *Communications of the ACM* 49, no. 4 (April 2006): 15–20, http://denninginstitute.com/pjd/PUBS/CACMcols/cacmApr06.pdf. *See* also Catherine B. Nelson, Jeannie A. Stamberger, and Brian D. Steckler, "The Evolution of Hastily Formed Networks for Disaster Response: Technologies, Case Studies, and Future Trends," (Conference Paper, IEEE Global Humanitarian Technology Conference, 2011). http://www.cisco.com/c/dam/en_us/about/doing_business/business_continuity/Paper_124_MSW_USltr_format.pdf.

[40] Fedwire, which is operated by the Federal Reserve Banks and authorized by the Federal Reserve Act, is just one example of this (legal authorities drawn primarily from 12 USC §§ 248(i),(j),248a,248-1,342). *See* LEGAL AND REGULATORY FRAMEWORK. Federal Reserve Banks, *Fedwire® Funds Service Disclosure* (Washington DC: WPO, December 24, 2015), 8–14, https://www.frbservices.org/ files/serviceofferings/pdf/fedwire-funds-service-disclosure.pdf. "U.S. law provides a comprehensive, well-established, and publicly disclosed legal framework for funds transfers made over the Fedwire Funds Service. The statutes, regulations, and contractual provisions that constitute the legal framework for the Fedwire Funds Service clearly define the rights and obligations of each party to Fedwire funds transfers. The legal framework provides participants a high degree of legal assurance of the settlement and finality of funds transfers made over the Fedwire Funds Service."

B. THE UNITED STATES AND CYBERSPACE

It is probable that, more than any other technological development over the last 100 years, the prolific spread of communications networks and information technology has presented an extraordinary number of challenges to a variety of prominent nation states,[41] and most especially the United States.[42] These more recent technological advances cannot be divorced nor entirely isolated from the crisis facing the nation state as a whole. Arguably, the emergence of cyberspace in the 1980s did not penetrate popular culture until the 1990s when the Internet grew into a household phenomenon,[43] but this did not stem the growth of cyber threats. For decades, cyber-attacks have consistently paralleled network advancements. All the while governing bodies have remained

---

[41] Sebastian Anthony, "France Looking at Banning TOR and Public WiFi," *ArsTechnica*, December 7, 2015, http://arstechnica.com/tech-policy/2015/12/france-looking-at-banning-tor-blocking-public-wi-fi. "According to leaked documents France's Ministry of Interior is considering two new proposals: a ban on free and shared Wi-Fi connections during a state of emergency, and measures to block Tor being used inside France. […] These proposals are presumably in response to the attacks in Paris [in November 2015] where 130 people were murdered." *See* also Keir Giles, "Russia's Public Stance on Cyberspace Issues," in *Proceedings of 2012 International Conference on Cyber Conflict*, eds. Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (Tallinn, Estonia: NATO CCD COE, June 5–8, 2012), 63–75, https://ccdcoe.org/publications/2012proceedings/CyCon_2012_Proceedings.pdf. "Russia has deep concerns on the principle of uncontrolled exchange of information in cyberspace." *See* also Hauke Johannes Gierow, "Cyber Security in China: New Political Leadership Focuses on Boosting National Security," *China Monitor of the Mercator Institute for China Studies* 20 (December 2014) http://www.merics.org/fileadmin/templates/download/china-monitor/China_Monitor_No_20_eng.pdf. "[China's cybersecurity] strategy defines a relatively broad range of objectives [which includes] tightening control of the internet to 'uphold good morals in the Net.'" *See* also *Wikipedia*, s.v. "Censorship of Wikipedia," last modified March 2, 2016, https://en.wikipedia.org/wiki/Censorship_of_Wikipedia.

[42] John Matherly, Twitter post, August 28, 2014, 10:49 a.m., https://twitter.com/achillean. Matherly (@achillean) posted an file created by web crawler SHODAN (https://www.shodan.io) that attempts to show all IPv4 devices connected to the internet for August 2, 2014. The data shows extremely high densities of devices for the United States and Europe though, interestingly, it is thought to have been inconclusive for China (due possibly to China's "Golden Shield Project"—a.k.a. the *Great Firewall of China*). The difficulty in comprehending, characterizing, and responding to threats in cyberspace is made more clear when glimpsing the sheer number of devices and vectors associated with the Internet. For further discussions on the Golden Shield Project, *see* generally *Wikipedia*, s.v. "Golden Shield Project," last modified February 28, 2016, https://en.wikipedia.org/wiki/Golden_Shield_Project.

[43] *See* generally Daniel Ventre, "Conclusion," in *Cyber Conflict: Competing National Perspectives*, ed. Daniel Ventre (Hoboken, NJ: John Wiley & Sons, 2012), 297.

relatively slow to respond—at least when compared to the pace of technological advancements and network proliferation.[44]

In light of this, it might surprise many that cyberspace has only recently emerged as a priority in discussions on national security. Its prevalence in discussions on security is another example of the increased awareness of national susceptibility and dependency on networks and information technology. Take, for example, the following descriptions coming from different organizations within the federal government, all addressing 21st century cyberspace threats:

> The 21st century brings with it entirely new challenges, in which criminal and national security threats strike from afar through computer networks, with potentially devastating consequences.[45]
>
> —Federal Bureau of Investigation

> Potential state and non-state adversaries conduct malicious cyber activities against U.S. interests globally and in a manner intended to test the limits of what the United States and the international community will tolerate.[46]
>
> —Department of Defense

[44] *See* INTERNET USERS IN THE WORLD. "Internet Users," Internet Live Stats, accessed January 20, 2016, http://www.internetlivestats.com/internet-users. Data provided by the International Telecommunication Union (ITU) suggests that there were just over 14-million internet users (or 0.3% of the world's population) in 1993. By the start of 2016, there are estimated to be over 3-billion users (or 40.5% of the world's population).

[45] *See* generally "Addressing Threats to the Nation's Cybersecurity," National Cyber Investigative Task Force, Federal Bureau of Investigation, accessed January 12, 2016, https://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity-1.

[46] U.S. Department of Defense, *The Department of Defense Cyber Strategy* (Washington DC: DOD, 2015) http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

> Cybersecurity is one of the most serious economic and national security challenges we face as a nation. Government systems—including Coast Guard systems—face a mounting array of emerging cyber threats that could severely compromise and limit our Service's ability to perform our essential missions.[47]
>
> —U.S. Coast Guard

> Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people.[48]
>
> —President George W. Bush

This recent emphasis by strategists and government leaders is unsettling and long overdue. Whether this awareness has appeared slowly due to the perceived "recent" nature of cyberspace is not entirely clear since cyber-attacks have a well-documented history as a dominant and disruptive force.[49] While the prominence of cybercrime[50] and espionage[51] has led to modestly effective

---

[47] *See* INTRODUCTION. Commandant of the U.S. Coast Guard, *United States Coast Guard Cyber Strategy* (Washington DC: DHS, June, 2015), 9, https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf.

[48] *See* Introductory Letter by President George W. Bush. U.S. White House, *The National Strategy to Secure Cyberspace* (Washington DC: White House 2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

[49] *See* generally *Wikipedia*, s.v. "Timeline of Computer Security Hacker History," last modified February 28, 2016, https://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history.

[50] *See* generally Internet Crime Complaint Center, *2014 Internet Crime Report*, Federal Bureau of Investigation (Washington DC: DOJ 2014) https://www.fbi.gov/news/ news_blog/2014-ic3-annual-report. *See* also Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime. Economic Impact of Cybercrime II* (McAfee, June 2014), http://www.mcafee.com/hk/resources/reports/rp-economic-impact-cybercrime2.pdf. In 2014, the FBI's Internet Crime Center (IC3) reported losses of over $800-million due cybercrime or cybercrime related incidences. This represents just a fraction of the more than $400 billion in costs incurred by the global economy due to cybercrime.

[51] *See* generally Ellen Nakashima, "Chinese Hack Of Federal Personnel Files Included Security-Clearance Database," *Washington Post* (June 12, 2015) https://www.washingtonpost.com/world/national-security/chinese-hack-of-government-network-compromises-security-clearance-files/2015/06/12/9f91f146-1135-11e5-9726-49d6fa26a8c6_story.html.

judicial and legislative measures,[52] technology continues to outpace holistic federal responses to the problem.[53] Regardless, the increasing pace of cyber-legislation communicates the prevailing view that cyberspace requires policies and laws that are unique from those constructed in the decades preceding it.

It is not only judicial and legislative procedures that have lagged behind in their response to cyberspace threats. Events of the last century continue to impose a dominant lens through which current policies are created, strategic priorities are set, and contemporary legal interpretation is adapted. From among the emerging voices of cyber-inclined philosophers and legal pundits, many predispose themselves toward successful 20th century strategies like deterrence[54] and consequently attempt to craft templates that are inspired—and sometimes restricted—by preconceived notions of how conflicts ought to progress and conclude.[55] Masked as the journey toward a new form of deterrence, it more often appears that its most commonly shared attribute is its

---

[52] *See* REGULATORY STRUCTURE. Christopher H. Sterling, Phyllis W. Bernt, and Martin B.H. Weiss, *Shaping American Telecommunications: A History of Technology, Policy, and Economics* (New York: Routledge, 2005), 30–33. "The reactive and ad hoc nature of court proceedings makes them a poor vehicle for formulating coherent regulatory policies. Relying on legislation to regulate industry […] also proved ineffective. The legislative process is notoriously slow and inflexible. Laws passed to regulate firms are difficult to change when the need arises. The fact that it took Congress years to substantially amend the Communication Act of 1934 is proof of the slowness of the legislative process."

[53] Daniel Ventre "Conclusion," 297–301. Specifically, Ventre hypothesizes that "delays between the emergence of cyberspace, the appearance of threats, and the introduction of cyberspace into defense policies highlights the contrast between aggressor and victim models […] The victim's reaction time is incompatible with the attacker's pace […] The State […] requires hierarchy, planning, and organization […] The attacker […] [has] no hierarchy [which enables] rapidity, reactivity and capacity for surprise action."

[54] Thomas C. Schelling, *Arms and Influence*, (New Haven: Yale University Press, 1966).

[55] For emerging views on cyber deterrence, *see* generally Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, eds. Franklin D. Kramer, et al. (Dulles, VA: National Defense University Press, 2009), 309. *See* also Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice," *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 103. *See* also Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington D.C.: The National Academies Press, 2010), 55–57. *See* also Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and The Feasibility of Deterrence Against Cyberattack," *Journal of Cybersecurity* (2015): 1–15, doi: 10.1093/cybsec/tyv003.

end goal—namely, conflict avoidance.[56] Theories on conflict avoidance, however, are steeped in approaches stemming from nuclear deterrence, but there is no clear indication that the critical elements of such theories have a one-to-one correspondence in cyberspace.[57] This strategic mismatch has not prevented the adaptation of outmoded methodologies and may be a significant contributor to operational ineffectiveness.[58] Shifting the focus to the desired outcome—namely conflict avoidance—can also cause policy makers and legislators to characterize cyberspace events inconsistently. Malicious activity in this domain is often upgraded or downgraded in order to substantiate the current strategy and claim that success has been achieved so long as conflict has been effectively avoided.[59] In these cases, however, combatting the underlying causality is disputable and one resulting phenomenon is the deluge of opinion,

[56] *See* THEORETICAL AND POLICY IMPLICATIONS. Vesna Danilovic, *When Stakes Are High: Deterrence and Conflict Among Major Powers* (Ann Arbor, MI: University of Michigan Press, 2002), 163–65. Conflict avoidance is, "for the most part, logically and empirically inseparable from" deterrence stability."

[57] *See* BARRIERS TO CYBERSPACE DETERRENCE. Clorinda Trujillo, "The Limits of Cyberspace Deterrence," *Joint Force Quarterly* 75 (4th Qtr., 2014), 47–49. *See* also Mark Pomerleau, "In Cyber Defense, Can Cold War-Style Deterrence Work?" *Defense Systems* (April 20, 2015) https://defensesystems.com/articles/2015/04/20/dod-cyber-deterrence.aspx. A successful deterrence strategy should necessarily produce an outcome that minimizes conflict or avoids it altogether. While cyberspace can almost certainly be folded into a broad strategy of deterrence, it is unclear whether brandishing or the use of cyberspace munitions can directly lead to this with the same hegemonic influence as nuclear weapons.

[58] *See* generally Michael Hayden, Jeffrey Eisenach and Mike Daniels, "America's Strategy for Cyberspace: Is it Working?" (lecture, American Enterprise Institute Global Internet Strategy event, Washington DC, October 27, 2015), https://www.aei.org/wp-content/uploads/2015/10/Transcript1.pdf.

[59] *See* generally Barack Obama, interview by Candy Crowley, *CNN*, December 21, 2014 http://cnnpressroom.blogs.cnn.com/2014/12/21/cnns-candy-crowley-interviews-president-barack-obama. President Barak Obama denied that the North Korean data intrusion against Sony Pictures constituted an act of war and recast the incident as "an act of cybervandalism." *But see* generally Office of Infrastructure Protection, *2015 Commercial Facilities Sector-Specific Plan* (Washington DC: DHS, 2015), https://www.dhs.gov/sites/default/files/publications/nipp-ssp-commercial-facilities-2015-508.pdf. The Entertainment and Media subsector is considered critical infrastructure and includes motion picture studios and broadcast media.

legislation, and policy that have yet to adequately address cyberspace operations in a way that makes it predictable and effective.[60]

Within this 20th century paradigm, technological advancements continue to pose significant difficulties to modern military operations and law enforcement. To complicate matters, they have also proved to be exceptionally challenging on the legislative front. The advances experienced by information technology over the past four decades have been fraught with as many illuminating successes as missteps. The last decade, in particular, has seen the U.S. government come under significant and increased scrutiny from the American public, U.S. government officials, the global media, and the international community for its participation and conduct in cyberspace.[61]

There are numerous events that stand as exemplars for this type of scrutiny. Atypical events like the Electronic Disobedience Theater (EDT) cyber counter-offensive—conducted by the Department of Defense (DOD)—demonstrated the degree to which the absence of cyberspace policy could lead to violations of federal law.[62] Criminal prosecutions like those against the founder of the Silk Road online anonymous marketplace called into question the extent and transparency with which federal agencies could cooperate in criminal

---

[60] *See* ONLINE DISINHIBITION EFFECT. Jose R. Agustina, "Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect," *International Journal of Cyber Criminology* 9, no. 1, (January-June, 2015): 42–43, doi: 10.5281/zenodo.22239. Deterrence strategies, which rely heavily on rational actors, fail to adequately address non-nation states, "lone-wolf" actors, and the emergence of cyber disinhibition. This statement is consistent with the scale and scope of cyberspace that allows for high gains at relatively low risks. *Cf. supra* note 36.

[61] *See* REACTION. *Wikipedia*, s.v. "Edward Snowden," last modified March 6, 2016, https://en.wikipedia.org/wiki/Edward_Snowden. *See* also "Wyden Slams Latest, Worse Version of Cybersecurity Bill," Ron Wyden press release, December 16, 2015, accessed March 9, 2016, https://www.wyden.senate.gov/news/press-releases/wyden-slams-latest-worse-version-of-cybersecurity-bill. Senator Ron Wyden (D-OR) has been outspoken in his criticism of CISA and the government's approval of, what he calls a "surveillance bill by another name."

[62] Chris Hables Gray, *Cyborg Citizen: Politics in the Posthuman Age* (New York: Routledge, 2002) 42–43.

investigations.[63] These examples are complemented by watershed events like the Edward Snowden media leaks[64] and have each called into question whether the government's role in conducting cyberspace operations falls ethically within the constraints of its legal framework.

While cyberspace challenges are admittedly unique, and while there is no clear consensus on what the role of government in cyberspace should be, the reality is that the threats from cyberspace continue to grow. In the absence of radical amendments to the powers of Congress and the president, a response to these mounting threats to national security cannot be abdicated and, from an authorities standpoint, must be addressed by the federal government as provided for in the United States Code.[65]

It is the contention of this thesis that since the United States Code was designed to provide a framework for federal conduct, embedded title authorities can be used in a mutually supportive way to responsibly execute the laws governing the functioning of the federal government. Supporting this is a long and well-established history of inter-title interactions that are focused on advancing the objectives of the United States through mutual cooperation. While there are a host of policies and procedures established by each organization to operate within their specific charter, the authorities delegated under the U.S.C.

---

[63] *See* generally *United States of America v. Ross William Ulbricht*, in *Criminal Complaint of S.D.C. NY* (2015), https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf. Ross Ulbricht was charged with violations of 18 USC §§ 1030,1956 and 21 USC § 846 based on investigations that heavily relied upon cyberspace operations. *See* generally, *id.* in *Court Transcripts of S.D.C. NY* (2015), 679–758, https://archive.org/stream/pdfy-6s57o3H70B1vH6bF/253361725-USA-v-Ulbricht-transcript-1-20_djvu.txt. Transcripts show that defense lawyers were critical of the means and methods—presently undisclosed to the public—used to identify the defendant as the online persona, "Dread Pirate Roberts". Additionally, there were insinuations that this multi-department effort, which included the Department of Homeland Security (DHS), Department of Justice (DOJ), and the Department of the Treasury (Treasury), did not possess the capacity for such operations and would have been required to receive assistance from government agencies whose charter may not have jurisdiction in the realm of domestic criminal activity. On May 29, 2015, Ulbricht was sentenced to life in prison without the possibility of parole.

[64] *See* GLOBAL SURVEILLANCE DISCLOSURES. *Wikipedia* s.v. "Edward Snowden."

[65] This statement is not intended to diminish nor exclude the powers or authorities of individual states—including tribal territories and others—to make provision for the security of their territories.

are primarily concerned with oversight and compliance requirements and fiscal controls to authorize operations by federal (and some state) organizations. As such, the creation of a cohesive framework that accounts for these stipulations would likely enable the effective consolidation of planning and execution requirements. An increased understanding of the operational compatibilities would better enable federal and state organizations to adjust, modify, and the create policies that are better suited to address their own interests and limitations.

C. THE UNITED STATES CODE

1. The U.S.C. and Relevant Authorities

For the purposes of supporting the proposed framework of Chapter IV, it is essential to introduce the main title authorities that are considered for inter-title cooperation. This section is not exhaustive, but provides appropriate boundaries for further development in later sections. The seven federal title codes and one state statute represent the main thrust for all subsequent inter-title discussions and they provide a limited—though substantial—subset of all title authorities leveraged by federal entities operating in cyberspace.

a. Title 6: Domestic Security

Title 6 of the United States Code is responsible for creating the Department of Homeland Security and assigning it the primary responsibility for preventing, investigating, and prosecuting terrorism within the United States. To do this, DHS is additionally tasked with reducing U.S. vulnerability to terrorism, which includes minimizing damage from and assisting in recovery efforts for any terrorist attacks that do occur.[66] Aside from terrorism concerns, it is charged with coordinating response efforts for national emergencies. In the course of carrying out its duties, it is responsible for ensuring that its efforts do not economically impair the United States nor violate the civil rights and civil liberties of U.S.

[66] 6 USC § 111

citizens. Though it is not specifically charged with heading up counterdrug efforts, its focus on counterterrorism makes it responsible for monitoring "connections between illegal drug trafficking and terrorism."[67]

b. Title 10: Armed Forces

Title 10 describes the role of U.S. armed forces and provides the legal framework for their roles, missions, organizational structure, and the unique laws that govern them. Interestingly, most crimes committed by members of the United States military are subject to the Uniformed Code of Military Justice where commanding officers are given substantial leeway in administering justice and the burden of proof is often based on a preponderance of the evidence.[68] For those concerned that inter-title operations may allow certain organizations to operate outside the purview of the U.S. federal court, this is not often an issue as the doctrine of dual sovereigns[69] provides some allowances for military members to be tried under both court systems. Within its legal framework, the title code also identifies each component of the armed services and outlines the roles and responsibilities of each service—excepting the Coast Guard, who have additional statutory functions under 6 USC and 14 USC. Title 10 also contains the Insurrection Act, which provides limited authorization for the president to deploy members of the armed forces and militia (i.e., the National Guard) to prevent revolts that threaten the sovereignty of an individual state or the United States as a whole.

---

[67] *Id.* at (1)(H)

[68] In the case of a trial by court-martial, the burden of proof is based on evidence that establishes guilt beyond a reasonable doubt pursuant to 10 USC § 851(c).

[69] *See* generally Adam J. Adler, "Dual Sovereignty, Due Process, and Duplicative Punishment: A New Solution to an Old Problem," *The Yale Law Journal* 124, no. 2 (November 2014) http://www.yalelawjournal.org/note/dual-sovereignty-due-process-and-duplicative-punishment-a-new-solution-to-an-old-problem. *See* also discussions on court systems, *infra* at Ch. 4 s. (C). *See* also TABLE 4. INTERNATIONAL AND DOMESTIC COURT SYSTEMS. *Infra* at Ibid.

c. Title 14: Coast Guard

The unique nature of the United States Coast Guard (USCG) led to their exclusive codification under Title 14. Relevant sections of this code grant broad authorities to the Coast Guard that allow them to perform foreign and domestic missions with limited authorities from a myriad of other title codes. They a critical part of homeland security efforts and are levied with authorities from both 6 USC and 14 USC in this role. Generally speaking, the Coast Guard is also a member of the armed forces, which justifies their use of 10 USC and 50 USC. They are also the enforcement arm for customs and border protection for the waterways and approaches to the United States, which necessitates additional authorities under 19 USC, 33 USC, 46 USC, and 49 USC. A consolidated list of the aforementioned title codes still falls short of complete as the Coast Guard is regularly concerned with at least 12 title authorities in the daily execution of their duties.

d. Title 18: Crimes and Criminal Procedure

Title 18 is divided into five major parts. The first is concerned with the nature and type of crime that constitutes federal crime. The statutes are wide-ranging over its more-than 120 chapters, which cover everything from illegal hunting to terrorism. The second part outlines criminal procedure, which includes relevant sections governing the rights of the accused, arrests, the conduct of trials, and the limitations of federal jurisdiction. The remaining three sections cover the federal prison system, juvenile affairs, and immunity considerations for federal witnesses. Succeeding discussions will primarily concern themselves with the first two parts of this specific code.

e. Title 28: Judiciary and Judicial Procedure

Seeing the need for enforcing federal statutory law and the decisions of the court, Title 28 details the organization of the courts and establishes the Department of Justice (DOJ). Within the DOJ, there are a number of federal enforcement agencies, including the U.S. Marshals and the Federal Bureau of

Investigation (FBI). The FBI has been chartered to respond to varying forms of cyber-crime as it pertains to federal law and even hosts an updated online listing of "Cyber's Most Wanted" criminals.[70] To do this, the FBI primarily uses authorities outlined in 18 USC and 28 USC.

f. Title 32: National Guard

Though the National Guard is a simple concept in theory, it is legislatively a more difficult organization to manage and account for. Under 10 USC § 311, it is considered the state's "militia" and its existence fulfills the constitutional requirements of the Second Amendment.[71] Each state has its own National Guard unit, which receives federal funding to retain personnel, and to train and equip them in behalf of the security of the state. These personnel can be activated along three lines of authority. The first is at the behest of the state governor who can call member of the National Guard into a State Active Duty (SAD) status. This can be done for various reasons, including disaster relief and Homeland Defense, but all activities are subject to state statutes and state funding. The second is activation under Full-time National Guard Duty. This status covers training, but the governor is also able to use these authorities, subject to presidential or Secretary of Defense approval, to use federal funding to activate these forces under limited instances under Title 32 authorities.[72] It is worth noting that in both previous examples, there are statutory exemptions to the Posse Comitatus Act[73] that are granted for activated forces so long as they remain under the control of the state governor. The last example is the activation

---

[70] *See* generally "Cyber's Most Wanted," Federal Bureau of Investigation, accessed February 12, 2016, https://www.fbi.gov/wanted/cyber.

[71] *See* generally U.S. Constitution, Amend. 2. "A well-regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed." *See* also 2ND AMENDMENT. Edward F. Cooke, *A Detailed Analysis of the Constitution*, 7th ed. (Lanham, MD: Rowman & Littlefield, 2002), 100. The state has the right to maintain an armed militia, which is presently fulfilled by the National Guard.

[72] Primarily pursuant to 32 USC §§ 502(f), 901, 902.

[73] For an examination of the Posse Comitatus Act (18 USC § 1385) *see infra* at Ch. 2 s. (C)(4)(c).

of the National Guard under Title 10 authorities.[74] This active duty status places National Guard elements under the control of the Department of Defense in support of federal operations. Forces activated placed on active duty are subject to restrictions imposed by Posse Comitatus and are able to be deployed to foreign theaters with fewer restrictions, but are extremely constrained in their domestic employment. Discussions in Chapter III will show that while these same forces respond to both state and federal requirements, the title authorities that govern them—SAD, 10 USC, and 32 USC—are designed to be mutually supportive.

g. Title 50: War and National Defense

Boasting 43 chapters and complemented by a nigh-as-lengthy appendix, Title 50 provides governing legislation for U.S. conduct in times of war and in matters pertaining to National Defense. Of the many issues addressed in Title 50, espionage, national security, emergency powers, nuclear weapons, and intelligence activities draw the most attention. More appropriate to current discussions, Title 50 legislation is responsible for creating the Central Intelligence Agency (CIA)[75] and the National Security Agency (NSA).[76] The statutory nature of stipulations surrounding foreign intelligence[77]—to include electronic surveillance—is of particular importance when considering the extent to which the aforementioned agencies can cooperate with agencies operating under other title authorities.

2. The U.S.C.: Perceptions and Controversy

Sanctioned inter-title cooperation in support of operations—cyberspace or otherwise—has tended to converge along the lines of information and intelligence. The most dramatic of these convergences stem from the findings of

[74] 10 USC §§ 331,332,333,334,12301(d),12302,12304,12406.

[75] 50 USC §§ 3035, *et seq.*

[76] 50 USC §§ 3601, *et seq.*

[77] 50 USC §§ 1801, *et seq.*

the 9/11 Commission[78] even though inter-title cooperation was by no means a novelty prior to the release of the report. Intelligence gathering and information sharing have been foundational to every significant government operation in recent history and do not appear to fluctuate based on the foreign or domestic nature of the threat. Almost as a necessary consequence, the United States has become increasingly familiar with inter-title reforms that challenge previously held norms in light of new and present contexts. The reason that inter-title reforms and inter-title operations appear locked in perpetual contention are many. The course of legislation, however, generally conveys a twofold purpose. On the one hand, legislation appears to fulfill national desires for effectiveness in responding to issues of national security and advancing national interests,[79] for example, the USA PATRIOT Act.[80]. On the other hand, it is necessary to assure the American people that the tenets of their democratic rule are being equitably preserved through the limitation of power, reasonable accountability, and an uncompromising adherence to law. The War Powers Resolution of 1973[81] is one of the most recent examples of this—excluding presently the vast quantity of Presidential Policy Directives (PPD), Executive Orders (EO), and the like.[82]

Whether this balance achieves a reasonable foothold in the past, present, or future conduct of our government operations is a tangential matter. It is, however, significant in one aspect in that it generates a great deal of controversy and skews perceptions with regard to the course and conduct—even the

[78] Thomas H. Kean and Lee Hamilton, *Executive Summary of The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, National Commission on Terrorist Attacks upon the United States (Washington DC: GPO, 2004), 10–11. Among other things, the Commission found that "management should have ensured that information was shared and duties were clearly assigned across agencies, and across the foreign-domestic divide." Ultimately these findings would lead to the creation of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004.

[79] *See* generally, U.S. White House, *The National Security Strategy of the United States, 2002* (Washington DC: White House, 2002). Specifically, the NSS outlines four enduring national interests: 1. "The security of the United States, […] allies and partners" 2. [The] U.S. economy." 3. "Universal values." And 4. International order […] that promotes peace, security, and opportunity."

[80] Pub. L. 107-56

[81] Pub. L. 93-148

[82] *See* THE PLACE OF POLICY. *Infra* at Ch. 3 s. (A)(1).

existence—of inter-title operations. Some misinterpretations are simply misdiagnoses that stem from confusing policy restrictions, like organizational charters or Executive Orders, for the title authorities themselves. For example, it is possible—especially in light of the Snowden media leaks—to examine the form and function of intelligence organizations and incorrectly assume that the restrictions that govern one agency are restrictions that govern all activities under Title 50. The NSA, CIA, Defense Intelligence Agency (DIA), and other federal organizations have unique capabilities and restrictions that are all leveraged under 50 USC to advance national interests.

Other misapplications stem from miscomprehending the extent of capabilities that are available under separate title authorities. This most commonly occurs when critics point out that organizations like the armed forces—governed by 10 USC—should not be conducting covert activities since those are authorized only under Title 50. This stance, however, fails to grasp the authorization for the military to conduct intelligence and traditional military activities that may be covert in nature. This also ignores cooperative agreements like those enabled by EO 12333 that promote full partnerships most prominently seen in the unified efforts of the National Security Agency/Central Security Service (NSA/CSS).

Feeding into this misinformation are the myriad of analogies that are generally intended to clarify narrow features of inter-title cooperation, but are often expanded and misapplied to aspects they were never intended to address. The oft-used analogy of numerous “operational hats” is commonly associated with compartmentalizing responsibilities in a way that arguably does more to

confuse than clarify.[83] To begin with, a literal conveyance of the analogy incites ridicule for the idea of a single person wearing two hats. The legitimacy associated with any resolutions originating from this "dual-hatted" authority can easily be preempted with skepticism and distrust, even if there is no indication of statutory misconduct. In another sense, it is often used to describe an expectation of trust, which anticipates that either one or the other will be used and that a combination of the two constitutes a conflict of interest. It is doubtful that the "multiple hats" analogy is anything but disruptive understanding the control, compliance, and fiscal challenges that need to be addressed in order to legitimize inter-title cooperation. As such, *parallel lines of authority* is a preferred idiomatic expression over multiple hats.

These few examples are by no means exhaustive and so the following discussions will attempt to identify some of the more commonly perceived "incompatibilities" that shape legal discussions and are often said to preclude inter-title cooperation. These perceptions and controversies fall along a number of lines, but a quick distillation usually reveals that they are rarely concerned with actual matters of law.

a. Organizational Incompatibilities

Some argue that gross disparities in information handling and methods of classification, and divergences in the end-goals of the complex consortium of

[83] *See* generally National Security Agency, *Cryptologic Almanac 50th Anniversary Series: The Central Security Service,* DOCID: 3575724 (Washington DC: DOD, 2002), https://www.nsa.gov/public_info/_files/crypto_almanac_50th/The_CSS.pdf (document was sanitized and declassified on June 12, 2009). In response to concerns over the uncertainty of President Richard Nixon's instructions to create a new National Cryptologic Command, then Secretary of Defense, Melvin Laird, appointed Vice Admiral Noel Gayler as the chief architect of what would be called the Central Security Service (CSS). "The phrase 'dual-hat' came to be used quite a lot at this time. Admiral Gayler now wore two, director of NSA and chief of the Central Security Service." The phrase "Dual-hatted" or "two hats" is attested to in numerous publications. *E.g.* Laurie A. Mulford, "Let Slip the Dogs of (Cyber) War: Progressing Towards a Warfighting U.S. Cyber Command," (master's thesis, National Defense University, Joint Forces Staff College, 2013), 56. *See* also U.S. CYBER COMMAND. Miranda La Bash and Christopher Landis, "Legal, Policy, and Organizational Impediments to the Protection of Critical Infrastructure from Cyber Threats," (master's thesis, Carnegie Mellon University, 2013), 24.

federal agencies and organizations will or should prevent their cooperation.[84] This argument is immediately one that appeals to concerns that are outside the scope of this paper. It is true that politics, ambitions, and a host of other factors may become destructive forces to effective cooperation, but these organizational ambitions are matters of policy[85] and do not affect cooperation from a legal premise. In this same vein, critics will identify restrictions based on the charter of a specific organization and expand those restrictions to every authorized operation under that same title. For example, the NSA and CIA have, as their principle function, the conduct of foreign intelligence and counterintelligence activities[86] but in practice, the functions given to each are unique. The CIA has extensive authorities and capabilities to conduct intelligence gathering, to influence and intervene in global events, and to evaluate and disseminate all-source intelligence.[87] The NSA has a distinctly different charter,[88] in which the CIA is subordinated to them in regards to Signals Intelligence (SIGINT) and the cryptography protecting U.S. communications. Both organizations operate under unique charters that comply with statutes governing War and National Defense (50 USC). Far from mandating that these agencies operate independent of one another, their distinctions from law create dependencies that require cooperation.

---

[84] *See* generally Morton H. Halperin, Priscilla Clapp, and Arnold Kanter, "Organizational Interests," in *Bureaucratic Politics and Foreign Policy, 2nd ed*. (Washington D.C.: The Brookings Institution, 2006), 25–61.

[85] *See* generally, Steven Aftergood, "Reducing Overclassification Through Accountability," *Federation of American Scientists, Secrecy News Blog,* October 6, 2011, http://fas.org/blogs/secrecy/2011/10/brennan_ctr_report. *See* generally Kenneth Lieberthal, "The U.S. Intelligence Community and Foreign Policy: Getting Analysis Right," *The John L. Thornton China Center at The Brookings Institute* (Washington DC: Brookings Institute, 2009), http://www.brookings.edu/~/media/research/files/papers/2009/9/intelligence-community-lieberthal/09_intelligence_community_lieberthal.pdf.

[86] EO 12333 s. 1.7

[87] Morton H. Halperin *et al*, "Organizational Interests," 34–35.

[88] *See* SUMMARY. U.S. Library of Congress, Congressional Research Service (CRS), *P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act*, by Elizabeth B. Bazan, RL34143 (2007), https://www.fas.org/sgp/crs/intel/ RL34143.pdf. Domestic wiretaps authorized under FISA are still for the expressed purpose of obtaining information pertaining to foreign intelligence.

b. Transparent versus Covert

Others contend that an increase in authorities will necessarily make certain overt actions covert and vice versa. This may require members of the U.S. military, who are uniformed and traditionally seen as the embodiment of overt action, to be "forced" into roles where they are conducting clandestine operations. Andru Wall, former legal advisor to U.S. Special Operations Command, incisively points out that an unacknowledged contributor is "the belief that intelligence operatives live in a dark and shadowy world, while military forces are the proverbial knights on white horses."[89] As with previously vetted concerns of organizational incompatibility, this is a matter of policy and preference that fails to affect legal conclusions. The legal authorities granted to the military are capable of equally supporting both overt and clandestine operations. The extent to which this complies with international law, while a legitimate concern, fails to fall within the boundaries of concern as they pertain to title authorities. Furthermore, the checks and balances that govern international law do not necessarily apply to the federal system of the United States except in instances where the government has chosen to subordinate domestic law. The extent to which broad subordination of federal law can be achieved under current international statutes can is a matter of ongoing debate.[90]

This is not to say that international law is ungermane to the discussion. Specifically, with respect to Title 10, it can potentially impose another layer of legal requirements that alter cyberspace behavior and add concerns that are not

---

[89] *See* generally Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Journal* 85 (2011): 88, http://harvardnsj.org/wp-content/uploads/2012/01/Vol-3-Wall.pdf. "The U.S. military consistently ranks at the apex of most-trusted institutions in the United States. This trust is critical to America's all-volunteer military and some even suggest the trust disparity between Congress and the military is one reason why Congress is loath to publicly attack military policies. David Hill, "Respect for Military Surges," *The Hill* (July 18, 2006), http://thehill.com/opinion/columnists/david-hill/8251-respect-for-military-surges. A 2009 Gallop poll found 82% of Americans have a "great deal" or "quite a lot" of respect for the U.S. military, versus only 17% who felt the same way about Congress. Lydia Saad, *Congress Ranks Last in Confidence in Institutions*, GALLOP (July 22, 2010), http://www.gallup.com/poll/141512/congress-ranks-last-confidence-institutions.aspx."

[90] Glennon, *supra* note 21.

purely determined by national interests. Arguments stemming from this perspective tend to form the rationale that seeks to exclude Title 10 activities from all others on grounds that the domestic codifications governing the armed services are seen as entirely subordinated to international laws regulating conflict. This assertion is entirely hyperbole when taken at face value and is excluded under most cursory examinations.

For example, the parceling of forces and authorities through domestic legislation is hardly under the purview of international law, not to mention the fact that many countries, as a norm, lack significant distinctions between forces used for domestic enforcement and those used for waging or responding to war. This and other incorrect assumptions regarding covert and overt activity are founded on ill-defined policies and a misconflation of U.S. and international laws that govern military responsibilities in conflict.

In those disputes that point to nebulous policy frameworks, it is first important to recognize that the military is not restricted from engaging in clandestine and other intelligence related activities as a subset of their traditional military authorities granted through Title 10.[91] Furthermore, their cooperation with other clandestine agencies and participation in covert activities—most notably authorized under 50 USC—does not place them outside the purview of legislated oversight bodies. Though it may induce uneasiness to the lay observer, there are considerable legislative frameworks and oversight committees that are equipped and adequate for determining which authorities have been leveraged in a given operation. More simply put, similar activities with similar effects can be authorized through numerous and different title authorities. In many cases, there is no need to need to restrict certain activity types to the confines of a single code.

[91] *See* THE LAW PERMITS WHILE CONGRESS ATTEMPTS TO RESTRICT. Wall, 92–108. "A careful analysis of the law and related legislative history shows how the law permits much of what Congress attempts to restrict with its stovepiped approach to oversight of the military and intelligence community." *See* also OVERSIGHT & COMPLIANCE. *Infra* at Ch. 4 s. (A).

Intelligence has frequently been at the center of these heated inter-title discussions. In 1991, the U.S. House of Representatives published a conference report on intelligence activities[92] addressing dilemmas that are common to inter-title cyberspace operations. As such, it is necessary to understand legal corollaries where cyberspace and intelligence activities share distinctions—namely covert action versus traditional military action. It is equally important to recognize that the perpetual struggles for power between executive and legislative authorities have led to considerable distrust between the two. The report illustrates this by noting the disagreement between executive and congressional leaders with regard to the restrictions imposed by reporting requirements associated with the carrying out of covert action. Regarding this disagreement, President George H.W. Bush wrote

> I am aware of your concerns regarding the provision of notice to Congress of covert action and the December 17, 1986 opinion of the Office of Legal Counsel of the Department of Justice, with which you strongly disagree primarily because of the statement that 'a number of factors combine to support the conclusion that the 'timely notice' language should be read to leave the President with virtually unfettered discretion to choose the right moment for making the required notification.[93]

The disagreements regarding congressional authority in the area of covert action have become only more contentious in light of 21st century operations. Congress has more recently alleged that the president will redefine "covert

[92] U.S. Congress, House, *Conference Report On the Intelligence Authorization Act for Fiscal Year 1991*, 102nd Cong., 1st sess., 1991, H. Rep. 102-166, http://www.intelligence.senate.gov/sites/default/files/publications/102166.pdf.

[93] *Id.* at 27.

action" as "traditional military action" in order to avoid congressional oversight.[94] This alleged circumvention is addressed later,[95] but for present discussions, these concerns do not adequately account for the numerous examples where military intelligence activities—as authorized by Title 10—are nearly identical to intelligence activities governed by Title 50.

Even though these concerns have a legal aspect to them, it is unlikely that they are explicitly restricted by the framework of the United States Code. Instead, potential clashes along these lines generally constitute perpetual disagreement over definitions and categories of actions that characterize legislative and executive interactions—often as merely a matter of principle.

c. International versus Domestic

Other lines of contention are often the result of an error in how key aspects of international and domestic law are understood. These disputes converge upon seemingly foundational mandates that are nearly impossible to account for in cyberspace and are therefore, by default, presumed to be unlawful. To begin with, these arguments generally exist beyond the inter-title concerns of the United States Code and instead are derived from *jus in bello* and *jus ad bello* laws governing international conflict.[96] A prominent example of this centers on those Geneva Conventions requiring military service members to wear distinctive

---

[94] *See* generally U.S. Congress, House, Permanent Select Committee on Intelligence, *Report to Accompany H.R. 2701, 'The Intelligence Authorization Act for Fiscal Year 2010,'* 111th Cong., 1st sess., 2009, H. Rep. 111-186, at 48–49, https://www.congress.gov/111/crpt/hrpt186/CRPT-111hrpt186.pdf. The committee noted that executive agents would categorize clandestine operations as "Operational Preparation of the Environment" (OPE) in order to distinguish them as "traditional military activity." They further note that "overuse of this term has made the distinction all but meaningless" and that "there are no clear guidelines or principles for making consistent determinations." They substantiate this claim by advancing comments from the Director of National Intelligence (DNI) who "himself has acknowledged that there is no bright line between traditional intelligence missions carried out by the military and the operations of the CIA."

[95] *See* INTELLIGENCE ACTIVITIES. *Infra* at Ch. 3 s. (A)(2)(e).

[96] *See* CYBER OPERATIONS. Office of General Council, "Law of War Manual," U.S. Department of Defense (Washington DC: DOD, June, 2015): 994–1009, http://www.defense.gov/Portals/1/Documents/pubs/ Law-of-War-Manual-June-2015.pdf.

identifiers when engaged in conflict.[97] Upon initial examination, an indiscriminate application of this mandate mistakenly overlooks the fact that these laws are primarily derived from international humanitarian concerns[98]—a subject for which there is little consensus with regard to cyberspace.[99] In the second place, a general survey of its application by the United States in the physical domains will reveal that military members are authorized by the U.S.C. to conduct overt offensive operations and to gather intelligence covertly in support of military operations, the latter of which may be done without the need for a uniform. In fact, the president and Commander in Chief of the Armed Forces, who is the ultimate authority in these operations, is not required to don a uniform even though he can potentially be detained and prosecuted under international laws governing war.[100] Far from insinuating that international laws are malleable and

---

[97] *See* generally Protocol Additional to the Geneva Conventions of August 12, 1949, and Relative to the General Protection Against Effects of Hostilities, June 8, 1977, art. 48, 1125 U.N.T.S. 3.

[98] Ibid. Article 48 specifically notes that the purpose of distinctive identifiers is for the protection of the civilian population and civilian objects.

[99] *See* TALLINN 2.0. "Research," Cooperative Cyber Defence Center of Excellence (CCDCOE), North Atlantic Treaty Organization, accessed March 15, 2016, https://ccdcoe.org/research.html. The *Tallinn Manual 2.0* has an expected publishing date in 2016 is purported to provide a more adequate examination of "the international legal framework that applies to […] cyber operations. The relevant legal regimes include the law of state responsibility, the law of the sea, international telecommunications law, space law, diplomatic and consular law, and, with respect to individuals, human rights law. Tallinn 2.0 also explores how the general principles of international law, such as sovereignty, jurisdiction, due diligence and the prohibition of intervention, apply in the cyber context."

[100] *See* generally Toni Pfanner, "Military Uniforms and the Rule of Law," *International Review of the Red Cross* 86, no. 853 (March 2004): 99–110, https://www.icrc.org/eng/assets/files/other/irrc_853_pfanner.pdf. Geneva Conventions and corresponding uniform regulations for most nation states indicate that the law desired to distinguish lawful targets from unlawful targets. Specifically, Article 48 of Additional Protocol I states that "in order to ensure respect for and protection of the civilian population and civilian objects, the Parties to a conflict are required at all times to distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly must conduct their operations only against military objectives." *Cf.* Karl Rauscher, "It's Time to Write the Rules of Cyberwar: The world needs a Geneva Convention for Cybercombat," *IEEE Spectrum*, November 27, 2013 http://spectrum.ieee.org/telecom/security/its-time-to-write-the-rules-of-cyberwar. *See* also INTRODUCTION. Gary D. Solis, "Cyber Warfare," *Military Law Review* 219 (Spring 2014): 1–3, http://www.loc.gov/rr/frd/Military_Law/Military_Law_Review/pdf-files/219-spring-2014.pdf. The word "cyber" is not found in the Geneva Conventions and it is doubtful whether those resolutions are able to envision the three layers of cyberspace that are susceptible to conflict. It is additionally unlikely that it can, in its current form, address the implausibility of effectively conducting warfare over and against Information Technology.

amorphous, this illustrates a more salient point. The *lex lata* of cyberspace is highly dependent on the extent to which established norms can be adapted to the actions and arena of cyberspace. As noted previously, however, there is enormous disagreement as to whether cyberspace activity—in part or whole—possesses adequate real-world referents. This is just one example, but there are several alleged mandates for which it is difficult to find a cyber-equivalent.

The first major comprehensive attempt to adapt norms from physical space into cyberspace came with the release of the *Tallinn Manual*.[101] As a NATO initiative, it has attempted—mostly unsuccessfully[102]—to establish norms and garner international consensus for cyberspace operations as they pertain to international law. In light of its limited acceptance, it should come as no surprise that most of its critics assert that it is broadly inadequate for generating standards that nation states can practically apply.[103]

There is undoubtedly significant progress being made in this area,[104] but even with these discussions present, the argument *a fortiori* is found in the fact that actions conducted in war are not the exclusive concern of those authorities delegated by 10 USC. Conversely, not all actions conducted under 10 USC are

---

[101] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).

[102] CCDCOE, *supra* note 99. In contrast to the original Tallinn manual, which merely addresses the infrequent cyberspace actions that rise to the level of armed attack, Tallinn 2.0 purports to address the significantly more common "malevolent cyber operations that do not rise to the aforementioned levels."

[103] *See* generally Noah Simmons, "A Brave New World: Applying International Law of War to Cyber-Attacks," *Journal of Law & Cyber Warfare* 4, no. 1 (Winter 2014): 63–65. *See* also CYBER ATTACKS AND NON-STATE ACTORS. Solis, 19–22.

[104] *See* generally United Nations, *Developments in the Field of Information and Telecommunications in the Context of International Security Resolution*, June 26, 2015, A/70/172, accessed March 9, 2016, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/172. This resolution establishes broad norms in the "field of information and telecommunications in the context of international security."

necessarily actions of war.[105] In simplest terms, the sections of USC 10 that are concerned with international law are just a small subset of everything addressed in that title code. The scope of what the president can do under Title 10 is broader than the concerns of international law and, in many cases, does not require the patronage of the international community.[106] From the perspective of the international community, international law governs actions under a jurisprudence that does not concern itself with whether domestically implemented legal frameworks were correctly utilized for a given action. From the perspective of the United States, any U.S. action that is subordinated to international law must be *intra legem*, irrespective of which title authority is responsible for the action.[107]

[105] *See* generally Wall, 119. The "distinction between merely altering computer code without asserting control or degrading function and actually assuming control or degrading functions is consistent with international law, which does not generally consider intelligence activities to be acts of war." *See* also SHAPE (PHASE 0) and DETER (PHASE 1). Chairman, U.S. Joint Chiefs of Staff, *Joint Operational Planning*, Joint Publication 5-0, Washington DC: CJCS, August 11, 2011: III-42. Phases 0 and 1 of the Joint Operational Phasing Model are planned and carried out by uniformed member of the armed forces, yet they hardly qualify as acts that reach the threshold of war.

[106] *See* generally Dambisa Moyo and Niall Ferguson, *Dead Aid: Why Aid Is Not Working and How There Is a Better Way for Africa* (New York: Farrar, Straus and Giroux, 2009), 29–47. *See* also Oliver Cunningham, "The Humanitarian Aid Regime in the Republic of NGOs: The Fallacy of 'Building Back Better," *Josef Korbel Journal of Advanced International Studies* 4 (Summer 2012): 101–26. Some more notable examples include the limited role of the UN in mandating or restricting military participation in humanitarian assistance and disaster relief. Although the UN is assigned the lead role in responding to international disasters, it relies entirely off of contributions in terms of finances and personnel.

[107] This viewpoint prefers a *dualist* approach to law. Even within this dualist framework, however, there is a *de facto* compliance that favors *monism*. This is most evident through the subordination of state actions to international law when it is recognized that they affect the international community.

d. Capability and Tyranny

Other voices raise concerns that increasing government capability in cyberspace would potentially legitimize the growing "surveillance culture"[108] and possibly lead to gross violations of constitutional rights like freedom of speech, personal privacy, and unlawful searches and seizures.[109] This too, while masquerading as a legal pitfall, is already addressed by current legislation. Operating appropriately under the *current* restrictions and allowances outlined in the United States Code will necessitate that operators adhere to all necessary controls—to include rules governing search and seizure, privacy, evidence, and other statutory procedure. In addition, it is important here to clarify that an increase in capability does not equate to a reduction in oversight. Most of the parent organizations previously identified have a long history of cooperation centered on supporting a variety of National Security objectives.[110] The idea that an increase in capability has led to widespread and accepted practices of

---

[108] *See* generally Tim Jordan, *Cyberpower: The Culture and Politics of Cyberspace and the Internet* (New York: Rutledge, 1999), 203–205. *See* also Bruce Schneier, "The Public-Private Surveillance Partnership," *Bloomberg Businessweek*, July 31, 2013 http://www.bloombergview.com/articles/2013-07-31/the-public-private-surveillance-partnership. *See* also Ana Marie Cox, "Who Should We Fear More with Our Data: The Government or Companies?" Guardian, January 20, 2014, http://www.theguardian.com/commentisfree/2014/jan/20/obama-nsa-reform-companies-spying-data. Concerns over surveillance and what constitutes surveillance as it applies to privacy laws has arguably emerged as the primary concern of the U.S. populace in terms of their participation and involvement in cyberspace.

[109] *See* generally Lizzy Finnegan, "CISA and The War on Privacy," *Breitbart,* November 10, 2015, http://www.breitbart.com/tech/2015/11/10/cisa-and-the-war-on-privacy. *See* also Dominic Basulto, "We've Outgrown the Traditional Notions of Privacy," *Washington Post*, February 12, 2015 http://www.realcleartechnology.com/2015/02/12/we039ve_outgrown_the_traditional_notions_of_privacy_25650.html.

[110] *See* EXAMPLES OF INTER-TITLE COOPERATION. *Infra* at Ch. 3 s. (A)(2).

neglecting constitutional rights does not have any enduring legitimacy in fact.[111] This refutation is obvious in numerous historical examples where significant leaps in capability—notably automatic weapons, precision munitions, air power, cyberspace, nuclear weapons, and space technology—were integrated into government operations without corresponding breaches of constitutional law.[112] There have undeniably been government activities that have violated law and overstepped authorities, but the burden of proof rests with the critics who must

---

[111] *See* APPENDIX. Lisa O. Monaco, "Re: to Department of Justice of Office of Inspector General's (OIG) A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008," message to Michael E. Horowitz, Inspector General of the U.S. Department of Justice, August, 24 2012, in *A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008*, Office of the Inspector General (Washington DC: DOJ, September 2012), https://oig.justice.gov/reports/2015/ o1501.pdf (document was sanitized and declassified on January 9, 2015). The National Security Division (NSD) found that the IG's findings supported that the FBI had "implemented it [FISA] targeting procedures with commendable deliberation, thoroughness, and professionalism." *But see* generally "In Re Production of Tangible Things [Redacted]," BR 08-13 (FISC, March 2, 2009), http://www.dni.gov/files/documents/0328/039.%20A4000915%20%20BR%2008-13%20%20Order%20(3-2-09)%20Redacted%2020140327.pdf (document was sanitized and declassified on March 28, 2014). Based upon the preponderance of noncompliance, a judge ordered the NSA to seek FISC approval of the court in each instance where they required queries against telephone metadata. *See* generally Trevor Timm, "Wall Street Journal Columnist Repeatedly Gets His Facts Wrong About NSA Surveillance," *Electronic Frontier Foundation*, November 27, 2013, https://www.eff.org/deeplinks/2013/11/wall-street-journal-columnist-gordon-crovitz-repeatedly-gets-his-facts-wrong-about. Critics who point out that IG findings indicate "systemic" violations of FISA by the FBI and NSA will find it difficult to prove that those violations were committed for reasons other than the complexity associated with understanding and applying it. Most violations were linked to inadequate training or negligence due to misinterpretations. The FISC ruling to restrict NSA collection addressed this same issue. While negligence presents legal dilemmas, these acts hardly qualify as sinister or malicious and were never apparently deemed to be criminal in nature. Subsequent reports show that improvements to training and greater oversight led to marked improvements in legal compliance. Had corrupt practices been a systemic norm, it is doubtful that the leaked (now declassified) IG reports would have annotated such concern for statutory compliance. *Cf.* NSA Director of Civil Liberties and Privacy Office, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, (Washington DC: DOD, 2014), http://www.dni.gov/files/documents/0421/702 Unclassified%20Document.pdf.

[112] With due regard to the Snowden media leaks, it remains questionable as to whether the NSA was ever doing anything that constituted a violation of constitutional rights. *Cf.* "Remarks By the President in a Press Conference," U.S. Office of the Press Secretary press release, August 9, 2013, accessed March 9, 2016, https://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference. In addressing the Snowden leaks publicly, the president focused on changes that align with American values and not apparently to correct behavior in response to illegal activity. *But see* generally Edward Snowden, "Open Letter to the Brazilian People," *Folha de S Paulo*, December 17, 2013, reprinted in *The Guardian*, December 17, 2013, http://www.theguardian.com/world/2013/dec/17/edward-snowden-letter-brazilian-people. In an open letter to the global community, Snowden bemoaned the surveillance capabilities of the United States—as opposed to giving concrete examples of violations—which he apparently viewed as the primary indictment against the U.S. intelligence community.

prove a link to systemic norms of ignoring laws governing oversight and compliance.[113] Therefore, it is assumed that frameworks for oversight and compliance are sufficient for each title authority, as determined by congressional legislators. If these frameworks are sufficient, then the integrity of the operation will not be diminished as additional authorities are added so long as compliance requirements are adhered to. To strengthen the argument further, an increase in cooperation between title authorities should incorporate additional bodies of oversight and lead to an increased ability to identify missteps, mishaps, and violations.

e. Industry Is Better Suited

Far from a legal concern, this controversy seeks to make moot, in its entirety, any argument for federal presence—inter-title or otherwise—in cyberspace. Concerns over trustworthiness and efficiency tend to anchor these arguments that propose an industry-first solution to cyberspace operations. In many ways, this is a false dilemma posed by those who see the presence of government as an "all-or-nothing" decision. To no surprise, industry is not excluded from providing assistance that positively affects national security and bolsters law-enforcement efforts. The extreme suggestion, however, that the government has no place in cyberspace whatsoever is hardly a palatable solution. Establishing and enforcing laws governing appropriate behavior, identifying and protecting natural rights, and providing for the defense of the nation is the exclusive responsibility of government. To suggest a deviation from oversight standards in the singular area of cyberspace—which cannot be reasonably isolated from critical areas of federal responsibility—is inconsistent with established norms. To further suggest that industry should be fully vested

[113] To the contrary, the Office of the Director of National Intelligence (ODNI) implemented transparency measures in 2014 to address civil liberty concerns. ODNI regularly consolidates and released sanitized and declassified material to the public via its website. *Cf.* "IC on the Record," Office of the Director of National Intelligence, accessed March 9, 2016, http://icontherecord.tumblr.com/search/IG+report. Creating an effective link between the government and systemic corruption under current oversight measures is untenable—barring the unlikelihood of a mass cover-up across every branch and at almost every level of government.

with this responsibility seems remarkably inconsistent with federal mandates. Additionally, the shift of national defense responsibilities to the corporate sector seems largely incompatible with the form and function of corporations.

Government organizations operating in cyberspace are presumably doing so under legislation that is clearly tied to those constitutional rights granted to each citizen. The corporate goals that govern industry, however, are not required to align with the U.S. Constitution and are most likely tied to the fiduciary responsibility they have to their stockholders. If the Snowden revelations were to be used to cast the government in a positive light, they would show, at the very least, that the federal government struggles to keep secrets from U.S. citizens and foreign governments alike. Though certainly an arguable position in terms of transparency and trustworthiness, U.S. industry would struggle to mount a convincing argument demonstrating a record with consistently upstanding ethics and unblemished conduct.

As to the advantage held by industry over government in terms of efficiency, a favorable determination is not awarded to the party that is most efficient. Even if industry were able to perform more efficiently and with better results, this does not make a less efficient government solution unreasonable. The leading branches of the government should strive to be efficient because it makes fiscal sense and is most often in the best interest of the nation, but their considerations for law and the lengthy legislative processes that accompany it are not grounds to disqualify them from providing services that fall under the patronage of the national interest.

3. The U.S.C. and Relevant Agencies

One of the additional tasks necessary for recommending a framework for inter-title cooperation in cyberspace is gaining a reasonable understanding of the major federal organizations operating there. An exhaustive list is unnecessary because it detracts from the main effort, which is to create a framework into which these organizations can be incorporated in order to effectively plan and

conduct cyberspace operations. Indeed, incorporating too many groups into the scenarios of Chapter V will make an overwhelming chore out of accounting for how each organization will contribute to the overall operation. Attempting to prioritize a long list of organizational capabilities and goals within the minutia of complex operations is something better left to a staff that is equipped to support that depth of analysis. For the purposes of these scenarios, simplicity will allow for greater focus on how cooperation can be enabled in an environment where the overlap between the broader goals of each organization must be assumed. On the other hand, enumerating too few of these cyberspace actors has a near opposite effect in that it can fail to adequately equip planners to understand what is possible under the current legal framework. The ultimate goal is to enjoin planners to a framework that allows them to understand and plan for inter-title operations. It is not intended to merely establish two cases of inter-title cooperation that can then be added to their playbook.

Concededly, there is considerable variability to constructing an appropriately representative cross-section of federal actors operating in cyberspace. The list that follows in this section is inadequate but deemed to be reasonable for the purpose of the framework and scenarios. Most of the organizations were chosen because they have been at the center of many perceived or actual controversies. Others were selected because their influence, while possibly less known, is undisputed as it relates to their place in the current U.S. cyber strategy.[114]

The Department of Homeland Security is arguably one of the most prominent centerpieces in these discussions. Concerns for homeland security

[114] *See* generally U.S. White House, *National Strategy for Information Sharing and Safeguarding* (Washington DC: White House, 2012), https://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf. *See* also *id.*, *The National Security Strategy of the United States, 2015* (Washington DC: White House, 2015). *See* also U.S. Library of Congress, Congressional Research Service, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, by John Rollins and Anna C. Henning, R40427 (2009), http://www.fas.org/sgp/crs/natsec/ R40427.pdf. *See* also "Cybersecurity in Congressional Research Service Reports," Bureau of Justice Assistance, accessed March 10, 2016, https://it.ojp.gov/PrivacyLiberty/reports/service/ 2336.

are nearly inseparable from U.S. government ambitions in cyberspace. In order to provide an adequate response to these security concerns, DHS operates the National Cybersecurity and Communications Integration Center (NCCIC),[115] which is composed of numerous teams[116] under authorities that are primarily delineated in Title 6. Another equally dominant figure that looms large in policy debates is USCYBERCOM's Cyber Mission Force (CMF), which operates primarily under 10 USC, and occupies a place that is just as prominent in terms of national security. In addition to the title authorities governing their military operations, they are also influenced by a myriad of codes and corresponding sections as they pertain to support to homeland security, intelligence activities, law enforcement, and National Guard units, the latter of which is addressed by 32 USC.

The FBI and their cyber-crime unit operate under 18 USC and 28 USC—among others—while the CIA and NSA cyber teams operate almost exclusively under 50 USC. Significantly less is known about the planned makeup of the cyber cadre, which is still under development by the USCG and the authorities granted to them by 14 USC. They are among the most unique cyberspace operators since their charge over the approaches to the United States and its littorals gives them aspects of both military authorities and law enforcement capability.[117] Each of these organizations will be expanded upon, and some of them will be incorporated into the following chapter containing the scenarios.

---

[115] Established pursuant to 6 USC § 148.

[116] *See* NCCIC MISSION. "National Cybersecurity and Communications Integration Center," U.S. Department of Homeland Security, accessed March 10, 2016, https://www.us-cert.gov/nccic. The three primary operational teams are the United States Computer Emergency Readiness Team (US-CERT), the Industrial Control Systems Emergency Readiness Team (ICS-CERT), and the National Coordinating Center for Communications (NCC).

[117] *See* STRATEGIC PRIORITY: ENABLING OPERATIONS. Commandant of the U.S. Coast Guard, *United States Coast Guard Cyber Strategy*, 27–29. Although no formalized organization chart for the USCG cyber cadre has been publicly disseminated, the strategy calls for the "[development of] a career path for Coast Guard cyberspace operations personnel to include recruitment, training, and retention, to create a professional cadre with specialized skills in cybersecurity, cyber intelligence, cyber law enforcement missions, cyber support to critical infrastructure, and cyber [effects] operations." *Note*: "cyber effects" include offensive capabilities.

There are other notable operators like the State Department's Office of the Coordinator for Cyber Issues (S/CCI), which represents the third pillar of U.S. National Security under 22 USC.[118] The United States Secret Service, transferred to DHS from the Treasury in 2003, has long been responsible for an amalgam of cyber operations that are critical to national security. These will not be discussed because, in the latter case, its functions are mostly accounted for by the other organizations, and in the former case, its current operational significance makes it a crucial yet mostly peripheral partner in the realm of cyberspace.

a. USCYBERCOM (10 USC & 32 USC)

Cyber Mission Force: Outlined in The DOD Cyber Strategy,[119] the Cyber Mission Force is composed of three major operational elements that are bolstered by a variety of support elements. They include the National Mission Forces, Cyber Protection Forces, and the Combat Missions Forces.

National Mission Forces: Projected to comprise 13 National Mission Teams (NMT), the National Mission Forces are organized with a primary focus on defending the United States, its allies, and their interests against "cyberattacks of significant consequence."[120] There is not a great deal of amplifying information on the specific roles or support structures, but one unique aspect to this operational unit is their goal to "train and partner with key interagency organizations"[121] in support of their mission. Specifically, the DOD Cyber strategy identifies cooperative efforts that integrate capabilities between

---

[118] *See* generally Ashley S. Boyle, *Fact Sheet: U.S.C. Title 10, Title 22, and Title 50*, American Security Project (Washington DC: American Security Project, 2012): 1, http://www.americansecurityproject.org/ASP%20Reports/Ref%200073%20-%20U.S.C.%20Title 10%2C%20Title%2022%2C%20and%20Title%2050.pdf. "Title 10, Title 22, and Title 50 of the United States Code (U.S.C.) comprise the legislative foundation of US National Security and its related agents. These pieces of legislation describe, structure, and constrain the operation of the country's national security agencies. They are also complex legislative structures."

[119] DOD, *supra* note 46.

[120] *See* generally *id.* at 24–25.

[121] Ibid.

government components like the "FBI, CIA, [and] DHS"[122] among other agencies. One of the main emphases of these integrated teams is to extend the range of options available to the president in the case of cyberattacks that place the United States at significant risk. Though no details are provided as to how these relationships are enabled, it is obvious that the regular functioning of these teams envisions inter-title cooperation as a foundational element.

Cyber Protection Forces: The Cyber Protection Forces comprises 68 projected Cyber Protection Teams (CPT). They are assigned the primary task of finding and disrupting cyberspace threats that extend into traditional cyberspace terrain, but includes critical threat networks that are distinct to weapons and space systems. These teams are not the primary defense but are designed as an augmentation force to defend "priority DOD networks." These forces appear to be the primary point of integration for Title 32 authorities. Public statements released by the National Guard indicate a growing effort to establish title-32 capable teams throughout the United States.[123] One of their major goals is to position cyber protection units so that they can adequately respond to emergencies within each of the Federal Emergency Management Agency (FEMA) response regions.[124] Under authorities present in 32 USC, it appears that cyber capabilities will soon be subject to State Active Duty laws and made available to governors responsible for state security. This effort requires a tremendous amount of coordination in terms of infrastructure, training, manning, and munitions. One of the major initial challenges to this inter-title cooperation is that, to some degree, the capabilities and limitations of these teams must be understood by a competent authority within each state governor's office.

---

[122] Ibid.

[123] Jon Soucy, "Guard Set To Activate Additional Cyber Units," *National Guard Bureau*, December 9, 2015, http://www.nationalguard.mil/News/ArticleView/tabid/5563/Article/633547/guard-set-to-activate-additional-cyber-units.aspx.

[124] *See* generally "FEMA Regional Offices," Federal Emergency Management Agency, accessed March 10, 2016, https://emilms.fema.gov/IS800B/lesson4/NRF0104190t.htm.FEMA identifies 10 response regions where offices provide "an interagency facility staffed by Emergency Support Functions in anticipation of a serious incident in the region or immediately following an incident."

Combat Mission Forces: Combat Mission Teams (CMT) are expected to total 27 teams distributed to provide cyberspace support to Combatant Commanders (COCOM). These forces are generally seen as the answer to expectations for a traditional military response in cyberspace. As discussed previously, the traditional distinctions from physical conflict do not easily translate to a cyberspace response. CMT support to combatant commands generates a myriad of questions for which there is no clear answer—foremost among them is how geographically constrained military commanders can effectively respond in a domain that is often described as "borderless."[125] Regardless, these teams are designed to integrate cyberspace effects in support of theater operational planning.

b. FBI (18 USC and 28 USC)

Computer Crime and Intellectual Property Section (CCIPS): As an agency under the Department of Justice, the FBI has primary responsibility for investigations and intelligence gathering within domestic jurisdictions. This tends to be a major source of consternation as it relates to their involvement in inter-title operations. One traditional perception is that organizations under other departments—most notably the DOD and DOS—are less concerned with constitutional integrity since it often provides only an auxiliary concern to the international focus that primarily characterizes their operational planning and execution. While this is likely true for operations preceding the 9/11 attacks, the prevalence of counterterrorism and its associated conflict irregularities have led to sweeping reforms in training across every department. The result has been a broadening of operational considerations under a variety of legal frameworks that address domestic vice purely foreign concerns.

---

[125] *See* CRITICISMS BASED ON A LACK OF BOUNDARIES IN CYBERSPACE. Philip Adam Davis, "The Defamation of Choice-of-Law in Cyberspace: Countering the View that the Restatement (Second) of Conflict of Laws is Inadequate to Navigate the Borderless Reaches of the Intangible Frontier," *Federal Communications Law Journal* 54, no. 2 (March 2002): 350–56, http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1299&context=fclj.

It is not surprising, therefore, that the FBI has become an indispensable asset to operations whose successes are dependent on correctly addressing significant domestic aspects. The FBI is intimately aware of the domestic thresholds for gathering evidence as well as restrictions as they pertain to domestic intelligence gathering. Many shudder at the thought of intelligence efforts in a domestic setting, but this is no different from police surveillance and requires justification through appropriate legal avenues. The FBI does not have a free pass to skirt domestic protections and it too must meet FISA requirements for investigations in the same way as every other intelligence agency. The CCIPS is subject to executive guidelines as typically provided for by the Attorney General. Its agents are critical to inter-title operations since their experience with cybercrime give them an intimate familiarity with operations as they pertain to privacy concerns and considerations of search and seizure.[126] Federal law gives the FBI authority to investigate federal crimes that are not exclusively assigned to another federal agency.[127]

c. CIA and NSA (50 USC)

The CIA remains one of the most controversial agencies under executive control. This sentiment usually corresponds to the reputation they gained in the 1960s and 1970s when they were linked to ill-fated attempts to overthrow the Cuban government through failed assassination attempts and the infamous Bay of Pigs incident.[128] Their assistance to Chilean insurgents, revelations about the MKUltra program, and growing unease of the legality of their activities led to a severe curtailing of their authorities in the 1970s. As later discussions will address, much of the current Title 50 legislation dealing with oversight controls stems from domestic behavior associated with executive powers from the

[126] National Cyber Investigative Task Force, *supra* note 45.

[127] 28 USC § 533

[128] *See* generally "Bay of Pigs Release," Office of the Chief Information Officer's Information Management Services, last modified August 2, 2011, http://www.foia.cia.gov/collection/bay-pigs-release. Consolidated reports detail Foreign Policy objectives and the development of anti-Castro Policies under executive oversight.

presidential administrations of John F. Kennedy through Richard Nixon. These powers were dramatically curtailed by the 1980s, though this did not move them beyond the scrutiny of Congress and the public—The Iran-Contra Affair being one of the more notable examples.[129] Recent revelations from the Senate Select Committee on Intelligence (SSCI) allege "abuses and countless mistakes" on the part of the CIA in overseeing their Detention and Interrogation Program that was widely publicized for its use of torture techniques.[130] Despite the controversy associated with CIA activity since their inception, they continue to play a critical role in activities and operations in support of intelligence activities. This includes, though is hardly limited to, cyberspace.

CIA cyberspace operations are more related to those of other agencies than is often assumed. The Iraq and Afghanistan wars, the general rise of counterterrorism operations, and reliance on drone operations all form an overlapping tapestry of inter-agency operations that are nearly impossible to conduct in isolation from the military or other intelligence agencies.[131] With the sheer amount of coordination that is required to conduct ongoing cyberspace operations, it is unlikely that the CIA is able—or desiring—to do so in isolation from the other U.S. entities operating there. Additionally, with their counterterrorism-focused target set, it is unlikely that they will experience any

---

[129] Lawrence E. Walsh, *Firewall: The Iran-Contra Conspiracy and Cover-Up* (New York: W.W. Norton, 1997), 17–19. In response to revelations on CIA activity in the Iran-Contra Affair accompanied by perceived abuses of executive power, Congress enacted the Boland Amendments, which restricted U.S. support to Nicaraguan Contras. The amendments even went so far as to prohibit the National Security Council (NSC) from providing assistance to the Contras.

[130] *See* FORWARD by Senator Diane Feinstein. U.S. Congress, Senate, Select Committee on Intelligence, *Committee Study of the Central Intelligence Agency's Detention and Interrogation Program*, 113th Cong., 2nd sess., 2014, S. Rep. 113-288, iii-ix, http://www.intelligence.senate.gov/ sites/default/files/documents/CRPT-113srpt288.pdf (document was sanitized and declassified on December 8, 2014). *But see* MINORITY VIEWS by Senator Saxby Chambliss. *Id.* at 520–52. *See* also Director of the Central Intelligence Agency, *CIA Comments on the Senate Select Committee on Intelligence Report on the Rendition, Detention, and Interrogation Program* (Washington DC: CIA, 2013), https://www.cia.gov/library/reports/CIAs_June2013_Response_to_the_SSCI_Study_on_the_Former_Detention_and_Interrogation_Program.pdf (document was sanitized and declassified on December 8, 2014).

[131] Robert M. Chesney, "Beyond The Battlefield, Beyond Al Qaeda: The Destabilizing Legal Architecture of Counterterrorism," *Michigan Law Review* 112, no. 2 (November 2013): 167–168, http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1036 &context=mlr.

significant decline so long as combatting the threat of terrorism remains central to U.S. national security.[132]

Due to the secretive nature of the CIA, information on updated methodologies and the exact nature of each directorate is not easily discerned. What is clear, however, is that the creation of the Directorate for Digital Innovation (DDI), announced in October of 2015, is focused on advancing the Agency's mission and vision through an improved cyber-capability.[133] As with nearly every other organization's cyber-emergence, this requires development of tradecraft and increased investment in cyber-infrastructure. Also notable is the assertion that the new directorate will "be a strong, agile partner with […] our Intelligence Community" to support national requirements.[134] Far from being merely lip service, this emphasis on cooperative efforts is part of an emerging reality that the convergence of intelligence activities is inseparable in many ways from cyberspace operations.

The NSA is no less controversial. Until the Snowden revelations, however, they had arguably remained free from the sort of scrutiny and criticism that has characterized the public's relationship with the CIA.[135] Ironically, these organizations are not nearly as dissimilar as many might expect. Certainly, the NSA is unlikely to engage in the sort of "cloak and dagger" activity that is generally associated with the CIA, but when it comes to cyberspace, there is no reason to think that the methodologies of these intelligence-gathering organizations should dramatically differ. One of the effects of the aforementioned Snowden media leaks, was the rise to prominence of the NSA's Tailored Access

---

[132] *See* COMBAT THE PERSISTENT THREAT OF TERRORISM. U.S. White House, *The National Security Strategy of the United States, 2015*, 9–10.

[133] Guy Taylor, "CIA Goes Live With New Cyber Directorate, Massive Internal Reorganization," *Washington Times*, October 1, 2015, http://www.washingtontimes.com/news/2015/oct/1/cia-goes-live-with-new-cyber-directorate-massive-i.

[134] *See* DIGITAL INNOVATION. "Offices of CIA: Digital Innovation," Central Intelligence Agency, last modified October 1, 2015, https://www.cia.gov/offices-of-cia/digital-innovation/index.html.

[135]

Operations (TAO) program. Little is known about this elite group of cyberspace operators, but open-source reporting indicates that TAO has been influential in the area of computer network exploitation (CNE)[136] and the Intelligence Community's recent push for transparency even has their division chief involved in speaking engagements.[137]

Whether these organizations take a leading role in offensive operations similar to the CIA's administration of the drone program and execution of "lethal covert activities,"[138] remains for the three branches of government to resolve. Even without this capability, it is almost assured that Title 50 organizations, like the NSA and CIA, will be contributing to cyberspace planning and supporting operations in their capacity as agencies for foreign intelligence.

d. DHS (6 USC)

Both government and businesses alike have come to rely heavily on cyberspace. In fact, it has become so central to daily operations that it is now depended upon in almost every major area of society—emergency preparedness, domestic law enforcement, and industrial operations. Providing protection for these and other systems is considered an essential part of economic resiliency and national security. These aspects of the U.S. society—and many more—are dependent on the reliability and functionality of infrastructure, which in turn is linked to a global IT infrastructure. The Department of Homeland Security is charged with protecting this "critical infrastructure" from physical and cyber threats. To do this, DHS has a number of teams and

---

[136] Andrea Peterson, "The NSA Has Its Own Team Of Elite Hackers," *Washington Post*, August 29, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers.

[137] *See* generally Kim Zetter, "NSA Hacker Chief Explains How to Keep Him Out of Your System," *Wired*, January 28, 2016, http://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system.

[138] *See* generally Micah Zenko, "Transferring CIA Drone Strikes to the Pentagon: Policy Innovation Memorandum No. 31" (Memorandum of the Council on Foreign Relations: Center for Preventative Action, April 16, 2013), http://i.cfr.org/content/publications/attachments/PIM_Drones_Zenko_Final_4_16_13.pdf.

coordination centers that are specifically designed to respond to attacks against U.S. critical infrastructure. The mission of DHS, possibly more than any other federal organization, demands ease of inter-title cooperation in order to effectively ensure safety for critical sectors of the United States.[139]

National Cybersecurity and Communications Integration Center (NCCIC): The NCCIC[140] acts as a centralized hub for the coordination of a multitude of cyberspace activities as they relate to national-level cybersecurity and communication protection. They coordinate information sharing between the public sector, private sector, other government agencies (both state and federal), and international partners to increase situational awareness and ensure that actionable tasking is delivered to the appropriate entity. Two primary roles where their efforts are critical include their responsibility for coordinating national responses to cyber incidents that are covered under the National Cyber Incident Response Plan (NCIRP) and providing assistance in initiating, coordinating, responding, and reconstituting critical National Security or Emergency Preparedness (NS/EP) telecommunications in non-emergency, emergency, and crisis situations. In addition, they play a significant role in monitoring many ongoing cyber operations in order to analyze responses, which assists in mitigation determinations and improves current and future recovery efforts. They are composed of four main branches: The NCCIC Operations & Integration (NO&I), the National Coordinating Center for Communications (NCC), the United

---

[139] *See* generally U.S. White House, *Presidential Policy Directive for Critical Infrastructure Security and Resilience/PPD-21* (Washington DC: White House, 2013). PPD-21 identifies 16 critical sectors of the United States for which the Department of Homeland Security "evaluates national capabilities, opportunities, and challenges in protecting critical infrastructure; analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure; identifies security and resilience functions that are necessary for effective public-private engagement with all critical infrastructure sectors; develops a national plan and metrics, in coordination with SSAs and other critical infrastructure partners; integrates and coordinates Federal cross-sector security and resilience activities; identifies and analyzes key interdependencies among critical infrastructure sectors; and reports on the effectiveness of national efforts to strengthen the Nation's security and resilience posture for critical infrastructure."

[140] *See* generally "N-Kick," U.S. Department of Homeland Security, last modified October 30 2009, http://www.dhs.gov/blog/2009/10/30/n-kick.The NCCIC acronym is most often pronounced "ən'-kik" and sometimes phonetically represented as "N-Kick."

States Computer Emergency Readiness Team (US-CERT), and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).[141] Though all four branches are critical, for the purposes of brevity only the latter two will be briefly expanded upon in any detail.

US-CERT: The US-CERT is responsible for a number of areas that generally aim to improve the Nation's cybersecurity posture. US-CERT enables this by coordinating the sharing of relevant cyberspace information as well as by identifying and managing cyber-risks to national security. They advertise an extensive cyber capability that is able to conduct advanced analysis on networks and digital media with a focus on identifying and neutralizing malicious activity that is directed at critical nodes on U.S. networks. To ensure rapid responses to impending threats, their team operates the National Cybersecurity Protection System (NCPS), which is responsible for providing "intrusion detection and prevention capabilities to covered federal departments and agencies."[142] As a department focused on attacks that may occur on U.S. soil, their enduring challenge is to execute their mission while protecting the constitutional rights of U.S. citizens. To do this, they operate within an extensive network of personnel who receive, develop, and distribute actionable information "to federal departments and agencies, state and local governments, private sector organizations, and international partners."[143]

ICS-CERT: In contrast to other elements of the NCCIC, the ICS-CERT is responsible for coordinating security through partnership in both the public and private sectors categorized according to four key focus areas. First, they are committed to maintaining *situational awareness* on behalf of Critical Infrastructure and Key Resources (CIKR) stakeholders. For example, in 2014, ICS-CERT worked with the FBI to provide classified briefings to industry

---

[141] *See* generally "National Cybersecurity and Communications Integration Center," U.S. Computer Emergency Readiness Team (US-CERT), accessed March 10, 2016, https://www.us-cert.gov/nccic.

[142] *See* NCCIC MISSION. Ibid.

[143] Ibid.

stakeholders and are also responsible for developing the Private Sector Clearance Program for Critical Infrastructure (PSCP)[144] to ensure that sensitive information is still able to reach those responsible for managing various aspect of public and private industry.[145] Additionally, they provide incident response and technical analysis for critical control systems. In another effort with the FBI in 2014, the team identified various sets of malware that were attempting to infiltrate critical U.S. infrastructure. These sophisticated threats were identified through the coordinated efforts of US-CERT, the FBI, and industry partners. In addition to providing detailed analytics on the threats, affected industries were provided with remote and on-sight assistance by ICS-CERT operators. They also conduct vulnerability coordination by receiving, consolidating, and distributing known or suspected vulnerabilities to researchers and vendors for mitigation or correction. Lastly, to add to a recurring theme amongst cyberspace operators, an expressed organizational goal is to develop and strengthen partnerships with "law enforcement agencies and the intelligence community and [coordinate efforts] among Federal, State, [and local] governments and control systems owners, operators, and vendors."[146]

e. U.S. Coast Guard (USC 14)

The U.S. Coast Guard may present one of the most intriguing cases for government operations in cyberspace. Under the Homeland Security Act of 2002 (Pub.L. 107–296), the United States Coast Guard was transferred to the Department of Homeland Security, but can leverage up to ten different title

---

144 *See* generally National Protection and Programs Directorate, *Privacy Impact Assessment Update for the Private Sector Clearance Program for Critical Infrastructure, PIA-020(a)* (Washington DC: DHS, 2015), https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-pscp-february2015.pdf.

145 *See* generally National Cybersecurity and Communications Integration Center, "Incident Response Activity," *ICS-CERT Monitor* (September 2014 – February 2015): 1–5, https://ics-cert.us-cert.gov/sites/ default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf. *See* also *id.*, "Coordinated Vulnerability Disclosures," 12–14.

146 *See* generally National Cybersecurity and Communications Integration Center, "Fact Sheet: Industrial Control Systems Cyber Emergency Response Team," accessed March 10, 2016, https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_ICS-CERT_S508C.pdf.

codes[147] depending on the nature of their activity. Under statutory authority, they "shall be a military service and a branch of the armed forces of the United States at all times."[148] In addition to this, statutes reserve the possibility of placing the Coast Guard under the authority of the DOD—specifically, subordinated to the Department of the Navy[149]—if Congress deems it necessary by declaration of war, or at the president's request. Under authorities derived from Title 6, the USCG has 11 distinct missions that are divided into *Homeland security* and *Non-homeland security* missions.[150] Under missions that pertain to homeland security, the USCG is authorized to protect ports, waterways, and provide coastal security as well as perform drug interdiction and other law enforcement.[151]

The extent to which the USCG is authorized to use cyberspace operations to provide these protections presents a significant legal dilemma since, based on previous discussions, it is unclear how their protection of the approaches to the United States will be applied in a domain that does not simply nor easily correlate to geographic domains. Furthermore, the Coast Guard is one of the few agencies that is authorized to enforce federal, international, and domestic laws.[152] In the case of counter-drug operations, Title 10 requires that the USCG provide "members of the Coast Guard who are trained in law enforcement and have powers of the Coast Guard under Title 14" for the purposes of "performing law enforcement functions" including making "arrests and […] [carrying] out searches and seizures" and other "law enforcement" duties.[153] This is a significant capability and yet it remains unclear how it directly translates to support in

[147] 6 USC, 8 USC, 10 USC, 14 USC, 18 USC, 19 USC, 21 USC, 33 USC, 46 USC, and 50 USC.

[148] 14 USC § 1

[149] *Id.* at § 3

[150] *See* generally 6 USC § 468

[151] The spectrum of law enforcement authorities available to the USCG include federal customs (pursuant to 14 USC, § 143 and 19 USC §§ 1401(1),1709(b)) as well as general federal law enforcement authority afforded to customs officers (pursuant to 19 USC § 1589(a)).

[152] Pursuant to 14 USC § 2 (expanded upon in 14 USC § 89).

[153] *See* generally 10 USC § 379. Jurisdictions pursuant to *id.* at § 374(b)(4)(A)

cyberspace. This counternarcotics example provides an illuminating example of what is possible since the assignment of law-enforcement capable officers does not exclude their colocation aboard ships for the purpose of cooperative cyberspace operations.[154] Unlike the other branches of the armed forces, which are restricted in their law enforcement capability,[155] the USCG is not subject to the Posse Comitatus Act.[156]

Preceding discussions are only moderately fruitful since the Coast Guard's Cyber Command (CGCYBERCOM) has, at the time of writing this, yet to release a definitive plan for organizing and structuring their *Cyber Cadre*. As the Sector Specific Agency (SSA) for the Maritime Transportation System within the Transportation Sector,[157] the Coast Guard is undoubtedly considering approaches to provide measures that ensure its security in and against all domains[158]—most relevant to present discussions is cyberspace—but their recently released USCG Cyber Strategy of 2015 is far from conclusive in terms of practical implementation and simply outlines the need for a "cyber workforce" in order to achieve their strategic priority of "defending cyberspace."[159] Even without a publicly available plan, it is not difficult to perceive the trajectory of the USCG cyber forces. Nearly four years prior to the release of their cyber strategy, CAPT John Felker, USCG, gave a briefing that indicated cyber-overlap between at least six different title authorities and the need for cooperation between the Intelligence Community (IC), the DOJ, DOT, DHS, and the DOD.[160] These

---

[154] As applicable to relevant law enforcement and counter drug operations (10 USC §§ 374(b)(4)(A),379)

[155] Except as provided for under the Insurrection Act (10 USC §§ 332, *et seq.*)

[156] *See supra* note 152.

[157] *See* ANNEX B. Office of Infrastructure Protection, *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, (Washington DC: DHS, 2010), 165–206, http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf.

[158] *See* EXECUTIVE SUMMARY. *Id.* at 1–12.

[159] *See* generally Commandant of the U.S. Coast Guard, *United States Coast Guard Cyber Strategy*, 23–25.

[160] *See* generally John Felker, *Driving Mission Execution*, (Washington DC: USCG 2011) http://www.dtic.mil/ndia/2011jointmissions/WednesdayFelker.pdf.

developments are part of a consistently resurfacing message that the future effectiveness of the cyber force is dependent on a broader understanding of capabilities and limitations within an operational model that prioritizes cooperation in support of inter-title operations.

4. The U.S.C. and Relevant Legislation

The previous section identified the major federal organizations and agencies operating in cyberspace. No less critical are the relevant laws and amendments that dictate roles, responsibilities, and restrictions for each of these organizations and, in some cases, cyberspace as a whole. Recommending a framework for inter-title cooperation will very much depend on the allowances and limitations outlined in these laws as well as an understanding of their chief aim. Similar to discussions immediately preceding these, an exhaustive list of laws is unnecessary—though tempting. The volumes of legislation, litigation, and legal interpretation that would need to be addressed is an undertaking for which the task at hand is not intended. Embarking on this errand would likely doom all subsequent efforts and, consequently, the simplicity of an inter-title framework would likely never materialize. The legislative actions that are addressed in this section will have to suffice, and the modest resolution they provide will have to be folded, no doubt, into the debate that continues to characterize inter-title discussions.

It is crucial to draw attention, once again, to the considerable amount of disagreement in this key area. There is little consensus on what an essential legislative portfolio should contain in order to enable definitive conclusions to be reached on matters of inter-title operations. Excluding relevant law is especially difficult in light of the far-reaching implications of legislation for state, federal, and international jurisprudence. For example, the National Defense Authorization Act (NDAA) is passed each year to authorize budget expenditures for the Department of Defense. The NDAA for Fiscal Year 2012[161] is of particular

[161] Pub. L. 112–81

interest because it also included provisions for the detention of military prisoners—as authorized under the Authorization for Use of Military Force (AUMF)[162]—and may have critical implications for cyberspace operations that are intended to "prevent any future acts of international terrorism against the United States."[163] It has, however, been excluded from a more thorough discussion because its use in enabling inter-title cyberspace operations, while intriguing, is likely too speculative. In fact, the following list was not chosen because of its provocative nature or even its completeness in addressing the subject matter. Rather, it was selected primarily because it constitutes landmark pieces of legislation that resurface in pertinent works and public debates on cyberspace, inter-title cooperation, or both. The truth of the matter is that there is no amount of legal knowledge that is sufficient for this task, but even still, these should provide substantive observations through which to comprehend the *corpus juris* as it relates to this subject.

The Insurrection Act of 1807 is one of the first pieces of legislation that recognized the need to relax federal restrictions during times where rebellion threatened the security of states or the sovereignty of state governments. Though local uprisings have not been a genuine concern of recent history, the 9/11 attacks and Hurricane Katrina disasters led to the transformation of this outdated legislation, in 2006, into a considerably powerful avenue for the executive power to exert federal influence in state territories.[164] Ultimately, these amendments were repealed in 2008, but they appear to have left an indelible mark on the expansion of executive powers. Though not associated with quelling insurrection, the Robert T. Stafford Disaster Relief and Emergency Assistance Act (*Stafford Act*) is seen as complementary to the Insurrection Act in the broad allowances it affords to the U.S. president in the deployment of the armed forces

[162] Pub. L. 107-40

[163] Pub. L. 107-40, § 2(a)

[164] Pub. L. 109–364, div. A, title X, § 1076(a)(1) was amended on Jan. 28, 2008 by Pub. L. 110-181, div. A, title X, § 1068(a)(1) to effectively revert back to the version as amended in 1956.

within state territories. This culminating piece of legislation first surfaced in the 1950s as the Federal Disaster Relief Program, which by 1986 had grown into a more substantive and predictable framework for federal responses to U.S. natural disasters. The provisions of this act have seen only marginal legislative changes over the last three decades, but increased reliance on federal aid for relief from natural disasters has led to many criticisms that point to the Stafford Act's ineffective relief responses coupled with generous increases in executive discretion. The counterbalance to this perceived executive overreach—most notably the Insurrection Act—is alleged to be exemplified in the Posse Comitatus Act (PCA), which provides a general prohibition against Army and Air Forces being used to enforce civil law.

Due primarily to concerns over national security in the wake of the 9/11 attacks, congressional legislators introduced and approved temporary laws that would temporarily increase executive authority while reducing constraints, especially with regard to domestic surveillance. The consolidated acts and amendments were signed into law under the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)[165] with most provisions being temporary and initially set to expire on December 31, 2005. This controversial act, which affected a dozen different title codes, was extended multiple times—including under the USA FREEDOM Act—with most of the substantive provisions having been renewed through 2019. An examination of the USA PATRIOT Act will also address three of its primary benefactors.

The first is the Foreign Intelligence Surveillance Act of 1978 (FISA).[166] This particular piece of legislation has come under intense scrutiny in the wake of the Snowden media leaks[167] as it has attempted to resolve complications presented by cyberspace in the area of foreign intelligence gathering. Public

[165] *See supra* note 80.

[166] Pub. L. 95-511

[167] *Supra* note 61.

responses to bulk collection and secret judicial proceedings have been responsible for a contentious debate that will arguably only intensify as cyberspace becomes a more entrenched to federal government concerns over national security.

The second is the Electronic Communications Privacy Act of 1986 (ECPA), which is commonly used to refer to both the Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act. In light of advances in technology and networked communications, the ECPA has generally been acknowledged as a necessary update to the Federal Wiretap statute of 1968.

The final benefactor of the USA PATRIOT Act is the Computer Fraud and Abuse Act (CFAA),[168] which, along with the ECPA, was enacted in 1986 to enable federal investigation and prosecution against the increasing number of criminals who were relying on information technology to commit crimes. The controversy surrounding the CFAA most often stems from its ambiguous language, which grants broad latitude for the inclusion of nearly every networked computer—including cell phones, tablets, and reading devices—into criminal investigations.[169]

Lastly, the Cybersecurity Information Sharing Act of 2015 (CISA)[170] was signed into law by President Barak Obama on December 18, 2015 as part of the Consolidated Appropriations Act (CAA) of 2016. The inclusion of CISA in this spending bill—under the broader Cybersecurity Act of 2015[171]—is almost as

---

[168] Pub. L. 99-474, 100 Stat. 1213.

[169] *See* INTRODUCTION. Orin S. Kerr, "Vagueness Challenges to the Computer Fraud and Abuse Act," *Minnesota Law Review* 94, vol. 1561 (2010) http://minnesotalawreview.org/wp-content/uploads/2012/03/Kerr_MLR.pdf. Kerr states that "the CFAA has become so broad, and computers so common, that expansive or uncertain interpretations of unauthorized access will render it unconstitutional. Such interpretations would either provide insufficient notice of what is prohibited or fail to provide guidelines for law enforcement in violation of the constitutional requirement of Due Process of the law."

[170] Pub. L. 114-113

[171] *Id.* at Div. N.

controversial as its content.[172] The legislation went through two years of revision amid congressional and executive concerns before being signed into law and thereby granting increased liability protection to private industry for information shared with the government. Each of these acts—The Insurrection Act, PCA, USA PATRIOT, FISA, ECPA, CFAA, and CISA—will be discussed in anticipation of legality questions that inevitably arise from certain cyberspace operations and some related restrictions to inter-title cooperation. Additionally, these laws, while by no means comprehensive, represent a relevant contribution to shaping and understanding U.S.C. discussions in subsequent chapters.

a. Insurrection Act (10 USC §§ 331, *et seq.*)

There are numerous statutory exceptions that grant the federal government lawful avenues for responding to criminal activity. Most of these exceptions have been granted to smaller organizations like the FBI or U.S. Marshals, and in almost every case, they exclude domestic intervention by the armed forces. In the earliest days following the founding of United States, federal forces provided an essential supplement to undersupplied state militias and local law enforcement in suppressing rebellions and insurrection. As such, Congress passed the Insurrection Act of 1807, which allowed the president to use the armed forces and militia—now 10 USC and 32 USC, respectively—to "suppress, in a State, any insurrection, domestic violence, unlawful combination, or conspiracy."[173] As mentioned previously, these authorities were significantly expanded under legislation passed in 2006. Those amendments were subsequently repealed in 2008. Should current authorities be lawfully invoked, it remains the president's prerogative as to whether to use the National Guard or armed forces to respond to the threat.

---

[172] Congress had only recently reconvened on January 5, 2016 before new legislation was introduced before Rep. Justin Amash, et al, introduced legislation for the repeal of the Cybersecurity Act of 2015. *Cf.* U.S. Congress, House, Committees on Oversight and Government Reform, *et al.*, *A Bill to Repeal the Cybersecurity Act of 2015*, 114th Cong., 2nd sess., 2016, H.R. 4350, https://www.congress.gov/114/bills/hr4350/BILLS-114hr4350ih.pdf.

[173] 10 USC § 333

In the case of cyberspace, this is extremely beneficial in terms of response options since cyberspace threats can often be effectively neutralized from remote locations. Mapping the cyberspace threat—as it applies to the Insurrection Act—to a physical counterpart that justifies a federal response of this sort, however, remains a murky undertaking. Whether this particular piece of legislation will experience any substantive changes to bring clarity to the murky waters of cyberspace is unknown. In the meantime, there continue to be a variety of attempts to map these key physical terms—insurrection, domestic violence, unlawful combination, or conspiracy—to their cyberspace counterparts.

A major effort in this area has been undertaken by the Air Land Sea Application Center (ALSA) in their multiservice manual on Defense Support of Civil Authorities (DSCA) that was released in 2015.[174] This jointly produced service manual identifies "cyberspace-related incidents" as events that may trigger a response pursuant to relevant sections of the 10 USC pertaining to the Insurrection Act. Even with the recognition that cyberspace events may trigger a military response, there are still significant hurdles to deploying the armed forces under the justification of insurrection. First, only cyberspace events that meet the criteria for insurrection events would authorize military mobilization. Given the disagreement on physical and cyberspace equivalents, this is almost assured to be met with controversy. Second, and closely related to the first, is the fact that cyberspace is prone to accommodate the circumvention of response protocols

[174] *See* generally Air Land Sea Application Center, *Multi-Service Tactics, Techniques, And Procedures for Defense Support of Civil Authorities (DSCA) (ATP 3-28.1/MCWP 3-36.2/NTTP 3-57.2/AFTTP 3-2.67)* (Joint Base Langley-Eustis, VA: ALSA, 2015), http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/atp3_28x1.pdf.

and tactics that can conceal the intentions of actions and prevent the threshold for the deploying a federal response from being reached.[175]

Another key feature of the Insurrection Act concerns its options for federal response, which tend to be highly compartmentalized. For example, in 10 USC § 331, the president is authorized to deploy federal troops—pending a request from the state governor—in order to quell an uprising, but there are still key distinctions in how the National Guard and armed forces are authorized to be employed. These distinctions are highly dependent on the disposition of both the state government and executive powers and their individual perceptions of the developing situation. In addition to these considerations, there are also title concerns since the National Guard enjoys the possibility of supplementing local law enforcement, while the military is to be strictly limited to being used in defense of the state. This brings up questions as to whether the armed forces, acting in defense of a state, may perform offensive operations or even investigate intrusion and attack sources for the purpose of subsequent prosecutions.

These concerns aside, the general progression for deploying resources follows a formal request from the state, in response to which the executive powers are required to issue a proclamation to "order the insurgents to disperse and retire peacefully."[176] If the proclamation requirement is at all applicable to cyberspace—for which there is considerable doubt—some consideration must be

---

[175] *See* generally Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security: Strategic Security in the Cyber Age* 4, no. 2 (Summer 2011) doi: 10.5038/1944-0472.4.2.1. The terms for cyber-espionage and cyber-attack appear to be used interchangeably even though they justify dramatically different responses under frameworks for domestic and international law. *See* also INTRODUCTION AND STATEMENT OF PROBLEM. Chris Brown, Desmond Lee, Colin Scott, and Daniel Strunk, *American Cyber Insecurity: The Growing Danger of Cyber Attacks*, Duke University paper (Durham, NC: Duke University, 2014), 1–2. http://hdl.handle.net/10161/8881. "In scholarly work on cyber-security there remains a tendency to conflate [the areas of cyber attack and cyber espionage]. This tendency is problematic because it obscures significant differences between these problems that may call for dramatically disparate policy responses. While both cyber espionage and cyber crime are certainly areas of concern for the United States, cyber attacks, since they involve network disruption and danger to critical infrastructure and financial markets, pose the most pressing threat."

[176] Pursuant to 10 USC § 334.

made for the “reasonable duration” of time that must be allotted for dispersing. Whether this is measured in minutes or micro-seconds, federal responders would have to be held in abeyance for some set period of time before deploying capabilities on behalf of the state. Timelines aside, the bigger issue seems to evolve from the unlikely possibility of issuing a decree in the first place. Extensive employment of automation, use of covert channels, and the lack of support provided by current protocols makes traditional channels for communication an unreasonable option. Additionally, the ability to deliver a proclamation to disperse will likely first require finding the responsible parties, which almost entirely defeats the purpose of proclamation in the first place. Even with these considerations, however, it is improbable that the difficulties associated with issuing a proclamation to cyberspace actors will constrain or disqualify the president from deploying an appropriate federal response. As such, once the president has determined by reasonable means that dispersion is unlikely, he may order the deployment of an appropriate federal response to protect the state against domestic violence and insurrection.

There are two other sections that deal with insurrection and they share some noteworthy similarities. These sections allow the president to initiate a federal response without the consent of the state. In the first instance,[177] responses are authorized if the threat within a state poses a threat to the enforcement of federal law. Since it is unlikely that a cyber-threat of this requisite magnitude will originate entirely within the state it threatens, the threat to federal authority will arguably occupy the lion’s share of justifiable responses. The second instance[178] allows for a federal response if a determination is made by the president that the nature of the “insurrection, domestic violence, unlawful combination, or conspiracy” is such that the execution of constitutional, federal, and state law is hindered and state and federal law enforcement efforts are obstructed. As the number of cyberspace-related federal legislation grows, the

[177] Pursuant to 10 USC § 332.

[178] Pursuant to 10 USC § 333.

justification for interfering in state affairs may also increase, which is an area that has received surprisingly little attention.[179]

b. The Stafford Act (42 USC §§ 5121, *et seq*.)

The Stafford Act is relatively straightforward in its intent. Inconsistent federal responses to natural disasters created laborious approval processes and gross inefficiencies in delivering aide to state and local governments to assist in relief efforts. To correct this, Congress legislated processes to deploy federal resources leading up to and following disasters. To monitor and respond to events of this nature, President Jimmy Carter issued an executive order in 1979 that created FEMA, which currently resides under the Department of Homeland Security. A federal network of national and regional centers works to prepare for and respond to any number of natural disasters that may affect states throughout the year. This focus on advanced planning encourages states to create detailed disaster preparedness and recovery plans.

From the perspective of authorities, the president has authorization to issue any number of declarations identifying a major disaster or state of emergency. Once a declaration has been issued, the federal response can be initiated and the president has statutory approval to deploy the National Guard or armed forces to assist the state in domestic disaster relief. This deployment of federal troops into the domestic sphere leads to at least three main title

[179] *See* generally Thaddeus Hoffmeister, "An Insurrection Act for the 21st Century," Draft paper from the *Selected Works of Thaddeus Hoffmeister* (Dayton, OH: University of Dayton, 2009), 5–6, http://works.bepress.com/thaddeus_hoffmeister/6. Hoffmeister is keen to point out that there is need for an "updated Insurrection Act that addresses both current and future challenges that are sure to arise as this country grows increasingly reliant on the Active Duty military for homeland security." He further notes the difficulty in "creating a finished product that maintains the necessary balance in federal-State responsibilities during a domestic crisis." His discussions, however, are entirely absent any explicit reference to cyberspace. *See* also DOMESTIC OPERATIONS. International and Operational Law Department, "Operational Law Handbook," 193–214. The OLH for 2015 does not adequately address cyberspace considerations for support to Domestic Operations except to refer to the Incident Annexes of the 2008 National Response Framework (NRF). *Cf.* Federal Emergency Management Agency, *National Response Framework*, 2nd ed. (Washington DC: DHS, 2013), https://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf.

considerations that are themselves dependent on the nature of the presidential declaration.

The first consideration is based on the issuance of a major disaster that comes at the behest of the state. In the initial stages of a disaster, state officials are typically responsible for activating the state emergency operations plan. If state and federal representatives determine that the Preliminary Damage Assessment (PDA) warrants it, the governor can request that the president issue a declaration *of a major disaster*.[180] In this case, the state must agree to cost sharing measures for federal assistance pursuant to provisions within the Stafford Act.

Similarly, a second avenue for federal response can closely follow the previously outlined process, but may result in a presidential declaration of an emergency.[181] Even though the PDA is still typically conducted by state and federal representatives, the president may choose, with or without the consent of the state governor,[182] to issue an emergency declaration that allows for federal resources to be deployed and, significant to present lines of examination, can include assets operating under Title 10 and Title 32. Considerations under this declaration and the next to be discussed can be closely tied to threats against critical infrastructure.

Lastly, the president may issue a declaration of defense emergency.[183] This is a typically a preemptive measure that allows the federal government to conduct work for no longer than 10 days on systems that are essential for the "preservation of life and property."[184]

---

[180] *See* generally Federal Emergency Management Agency, "National Response Framework: Stafford Act Support to States," accessed March 10, 2016, https://www.fema.gov/pdf/emergency/nrf/nrf-stafford.pdf.

[181] Ibid.

[182] If issuance of an emergency declaration is absent the consent of the state governor, the federal government must determine that it has primary response authority pursuant to 42 USC § 5191(b).

[183] *See* FEMA, *supra* note 180.

[184] Pursuant to 42 USC § 5170b(c)(1).

All of these measures may appear clear-cut and benign within the grander narrative surrounding federal involvement in cyberspace operations. In one of the broadest interpretations of disaster relief, however, through policy interpretations, the executive powers have delineated extensive responsibilities to the DOD, DOJ, and DHS in declarations of "national security emergencies" that include "natural disaster, military attack, technological emergency, or other emergency, that seriously degrades or seriously threatens the national security of the United States."[185]

The broad authorities that this translates into can easily enable a spectrum of inter-title operations in support of emergency declarations under the Stafford Act. Rapid constitution of networks in support of technological emergencies can leverage members of the National Guard or military to re-enable banking, power restoration, communications, and coordinate search and rescue operations. This context can easily be aligned with the tiered approach to disaster response that is proposed by the 2008 National Response Framework.[186] The executive power in responding to "national emergencies" may be extensive, but it is important to remain cognizant of the fact that none of the provisions under the Stafford Act provide statutory exception for the Posse Comitatus Act—to be discussed in greater detail in the immediately succeeding section. The doctrine of the DOD is of particular interest in the context of these tensions and is often scrutinized as an attempt to circumvent restrictions imposed by the aforementioned act.[187] Despite the claims and the accompanying demands to revamp the Insurrection

---

[185] *See* generally 42 USC § 5195. *Cf.* EO 12656, "Assignment of Emergency Preparedness Responsibilities" (most recently amended under EO 13603 s. 803(a)).

[186] *See* generally Mark M. Beckler, "Insurrection Act Restored: States Likely to Maintain Authority Over National Guard During Domestic Emergencies," (monograph, United States Army Command and General Staff College, 2008), 50–56, http://www.dtic.mil/dtic/tr/fulltext/u2/a484794.pdf.

[187] *See* DISASTER RELIEF LAW: THE STAFFORD ACT. Isaac Tekie, "Bringing the Troops Home to a Disaster: Law, Order, and Humanitarian Relief," *Ohio State Law Journal* 67, no. 5 (2006): 1244–1246, http://hdl.handle.net/1811/71058. "The [Stafford] Act does not enable the military to restore law and order by arrests and seizures, nor by any other direct law enforcement methods unless those actions happen to consist of a military purpose like guarding military bases."

Act, Stafford Act, and Posse Comitatus Act, legal opinion has yet to side with this more insidious interpretation.[188]

c. Posse Comitatus Act (18 USC § 1385)

The PCA has long been seen as the quintessential legislation that balances the tendency for executive overreach. The phrase *posse comitatus* is Latin for the "force of the county" and generally refers to a group of citizens who are called upon to defend the territory or "county" in a law enforcement role.[189] The United States in particular has a general prohibition against presidential use of the armed forces or National Guard for the purposes of law enforcement.[190] The specifics of the legislation prohibit the use of "Army or the Air Force as a posse comitatus or otherwise to execute the laws." Although the United States Navy and Marine Corps are not explicitly included in the prohibition of PCA, they were made subject to it under DOD regulation beginning in 1992.[191] The PCA, while effective at providing broad prohibitions against the use of the armed forces

---

[188] *See* NOTE 105. *Id.* at 1245. "DOD DIRECTIVE 5525.5 para. E2.1.4 (1986). The military purpose doctrine is not an exception to the PCA because actions undertaken for a valid military purpose fall outside the scope of the purpose of the PCA to prohibit military enforcement of civilian laws. People v. Burden, 303 N.W.2d 444, 447 (Mich. 1981); Clarence I. Meeks III, *Illegal Law Enforcement: Aiding Civil Authorities in Violation of the Posse Comitatus Act*, 70 MIL. L. REV. 83, 124 (1975). Any benefits provided to civilian law enforcement pursuant to a military purpose are said to be incidental to the primary purpose. *Id*. at 124–26. […] the obvious question for the courts, which generally arises when military actions provide law enforcement benefits, is what constitutes a valid military purpose? The answer given by courts escapes consistency. *See* [Charles Doyle, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law*, in THE POSSE COMITATUS ACT AND RELATED MATTERS: CURRENT ISSUES AND BACKGROUND 17, 24 (Susan Boriotti & Donna Dennis eds., 2004)]: 49–51. Stricter courts demand a close nexus between the stated purpose and the law enforcement activity, while others settle for a mere relation between the two. *Id.* Notably, these cases arise in activities like undercover drug operations and routine criminal investigations. The working of this exception in the context of a large-scale disaster relief effort is not covered by the cases."

[189] Bryan A. Garner, ed., *Black's Law Dictionary*, 9th ed. (St. Paul, MN: West Group, 2009) s.v. "Posse Comitatus." Defined as "The power or force of the county. The entire population of a county above the age of fifteen, which a sheriff may summon to his assistance in certain cases, as to aid him in keeping the peace, in pursuing and arresting felons, etc."

[190] *See* NOTE 11. Matthew Carlton Hammond, "The Posse Comitatus Act: A Principle in Need of Renewal," *Washington University Law Quarterly* 75, no. 2 (1997): 954, http://openscholarship.wustl.edu/law_lawreview/vol75/iss2/11. "In 1854, the Attorney General interpreted posse comitatus to include the military." *See* NOTE 44. *Id.* at 960. "Act of Sept. 18, 1850, ch. 60, 9 Stat. 462,462-63."

[191] 32 C.F.R. § 213.2

in the employment of domestic law enforcement, still falls short in a number of areas.

There are numerous examples of congressional legislation that effectively create statutory exceptions to the PCA.[192] For one, the National Guard when under the control of the state governor—SAD status—can fill key law enforcement roles and the armed forces can respond to national security concerns over nuclear, chemical, and biological threats.[193] The Coast Guard has already been noted as being exempt from PCA and there are numerous Title 10 exceptions, like those that require the armed forces to "serve as the single lead agency" for surveillance against "aerial and maritime transit of illegal drugs into the United States."[194]

Since Title 10 is the primary object of PCA, it is worth enumerating the extensive authorizations that are at least tangentially concerned with statutory compliance. Title 10 has been modified over the course of its existence to enhance cooperative efforts with state authorities in support of operations not strictly prohibited by the Posse Comitatus Act—but also not restricted to the provisions of the Insurrection Act and the Stafford Act.[195] The armed forces are given broad latitude to assist in cases of domestic emergencies[196] to share information with federal, state, or local law enforcement officials,[197] and to "make

---

[192] *See* APPENDIX A – Notable Violations and Exceptions to the Posse Comitatus Act. *See* also APPENDIX D. Eric V. Larson and John E. Peters, "Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options," (monograph report, Rand Corporation, 2001), 243–45, http://www.rand.org/pubs/monograph_reports/MR1251.html.

[193] 18 USC §§ 831,832. § 832 still has restrictions against arrests made by federal troops.

[194] 10 USC § 124

[195] Pursuant to USC 10 §§ 380,381.

[196] USC 10 § 2557 allows the DOD to provide "excess nonlethal supplies: availability for humanitarian relief [and] domestic emergency assistance," which could easily include cyber infrastructure. This reasonable provision could be provided pursuant to USC 10 § 2557(c) so long as the military does not "conduct any activity which, if carried out as an intelligence activity by the Department of Defense, would require a notice to the intelligence committees under title V of the National Security Act of 1947 (50 U.S.C. 3091, et seq.)."

[197] Only information that was gathered during the normal course of military training or operations may be shared with state and local law enforcement. This information has the added stipulation that it must be relevant to a violation of federal or state law pursuant to 10 USC § 371.

available any [DOD] equipment […] [or] base facility […]"—presumably cyberspace infrastructure is included—"to any Federal, State, or local civilian law enforcement official for law enforcement purposes."[198] Title 10 further allows DOD to train local law enforcement on operating and maintaining this equipment[199] and to make DOD personnel available for operating this equipment.[200] These allowances are available through inter-title cooperation with other federal agencies[201] and civilian law enforcement.[202]

Far from establishing broad principles for undermining the intent of the PCA, these exceptions provide demarcation lines that limit federal military power to a *passive* role that is intended to reinforce state—vice federal—objectives with restrictions that prevent supplanting local law enforcement efforts.[203] These passive allowances are followed up by appropriate limitations that prohibit the

---

[198] 10 USC § 372

[199] 10 USC § 373

[200] Subject to restrictions pursuant to 10 USC § 374.

[201] *See* generally 10 USC § 374(b)(1). Under the general provisions of this section, the Secretary of Defense may make DOD personnel available to another federal agency for the maintenance and operation of equipment with respect to select criminal violations and in support *that agency's support* to foreign, state, or municipal governments. This includes support of "a foreign or domestic counter-terrorism operation" as well as "the rendition of a suspected terrorist from a foreign country, and other activities" so long as "such support does not involve direct participation by such personnel in a civilian law enforcement operation unless such direct participation is otherwise authorized by law."

[202] *See* generally 10 USC § 374(b)(2). Under the general provisions of this section, the Secretary of Defense may make DOD personnel available to "a civilian law enforcement agency" for the purposes of "detection, monitoring, and communication of the movement of air and sea traffic," and specifically the "movement of surface traffic outside of the geographic boundary of the United States and within the United States not to exceed 25 miles of the boundary if the initial detection occurred outside of the boundary." They are additional authorized to provide personnel support for "aerial reconnaissance" and the "interception of vessels or aircraft detected outside the land area of the United States for the purposes of communicating with such vessels and aircraft to direct such vessels and aircraft to go to a location designated by appropriate civilian officials." DOD personnel may ultimately operate equipment "to facilitate communications in connection with specified law enforcement programs" and in other cases pursuant to 10 USC § 374(b)(4) to the extent that "such support does not involve direct participation by such personnel in a civilian law enforcement operation unless such direct participation is otherwise authorized by law."

[203] *See* THE POSSE COMITATUS ACT. Danielle Crockett, "The Insurrection Act and Executive Power to Respond with Force to Natural Disasters" (Paper prepared for Law 224.9: Disasters & the Law, University of California Berkeley School of Law, 2007), 20–26, https://www.law.berkeley.edu/library/resources/ disasters/Crockett.pdf.

"direct participation by a member of the [armed forces] in a search, seizure, [or] arrest […] unless […] such activity by such member is otherwise authorized by law."[204] These limitations are also complemented with fiscal restrictions that require reimbursement by any agency that receives or utilizes these services.[205]

Along the lines of PCA compliance it is important to note that the courts have regularly determined that the Posse Comitatus Act is generally held to have been violated in the absence of a recognized exception. This specifically applies when local law enforcement employ military investigators—termed "direct active use"—or "when the use of the military 'pervades the activities' of the civilian officials" or subjects "citizens to the exercise of military power that is 'regulatory, prescriptive, or compulsory in nature.'"[206] In terms of implications for cyberspace, this likely means that military forces will be relegated to a passive role—unless employed under authorities pursuant to the Insurrection Act or Stafford Act—in providing infrastructure and training, but not in active implementation of state cyberspace efforts—most importantly those cyberspace efforts that relate to law enforcement. Their regular and positive contribution should allow fiscally constrained state governments to utilize DOD infrastructure to provide a level of

[204] 10 USC § 375

[205] Where federal reimbursements are not explicitly linked to specific agencies and organizations, they generally fall under the statutory authority of the Economy Act (31 USC § 1535)

[206] U.S. Library of Congress, Congressional Research Service, *The Use of Federal Troops for Disaster Assistance: Legal Issues*, by Jennifer K. Elsea and R. Chuck Mason, RS22266 (2008), 1–2, https://www.fas.org/sgp/crs/natsec/RS22266.pdf.

security that aligns with citizens' constitutional rights and state statutory authority.[207]

It is worthwhile to end PCA discussion with some affirmative statements regarding the extent to which it affects specific title authorities. The stipulations on Title 10 activities have been covered to a reasonable degree, but the Act does not generally apply to the National Guard while they are in a SAD status, which allows them to be used for law enforcement purposes, nor does it apply to them while activated under 32 USC authorities. Conditions of the PCA are not applicable to FBI operations (18 USC) in investigating and prosecuting cybercrime nor do they hold authority over the Coast Guard (14 USC) when operating in a peace-time capacity[208] or DHS (6 USC) in the execution of homeland security operations. Since the CIA and NSA (50 USC) do not have a law enforcement role, PCA is unlikely to influence their involvement, which typically requires the elements foreign intelligence or counterterrorism to be present.[209]

---

[207] *See* Crockett, 24–25. Crockett illuminates many arguments purporting to undermine the intent of the PCA. For example, "DOD Directive 5525 § E4.1.2.3 (1989)" is cited as providing "the inherent right 'to ensure the preservation of public order and to carry out governmental operations within its territorial limits, or otherwise in accordance with applicable law, by force, if necessary.'" Further, DOD Directive 3025.1 § 4.5 (1993) and 32 C.F.R. § 215.4(c)(2)(ii) allow commanders to "provide resources and assistance, including law enforcement, when a disaster overwhelms the capabilities of State authorities and requires an immediate response." Crockett maintains, however, that "the PCA's requirement of 'an Act of Congress' indicates that the Department of Defense does not have the authority to create exceptions to the PCA." She supports this by noting DOD Directive 3025.1-M, C8.5, at 109 (June 1994), which "states that [the directive] is not to be relied upon as a source of authority and instead should be viewed as providing guidance." This manual, she notes, "identifies the Posse Comitatus Act as a limitation on the military's role in disaster response" and cites DOD regulations, which "explicitly state that only the President (or the Attorney General if authorized by the President) may request the use of active duty military forces in response to domestic disturbances."

[208] Wartime obligations are unlikely to supplant the USCG's role in homeland security operations pursuant to relevant provisions within 6 USC, 14 USC, et al.

[209] Although NSA is subordinate to the DOD and managed by military staff, they are not generally acknowledged to be constrained by this particular Act since those organizations that constitute the armed forces are the explicit object of the PCA's federally imposed limitations. An argument *a fortiori* is found in the exemptions to a number of federal limitations as provided for in the USA PATRIOT Act and FISA, which fulfill the clause that takes exception to those "cases and […] circumstances expressly authorized by the Constitution or Act of Congress."

Later discussions will address the need for considering the effectiveness of each of these organizations and the context that determines which legislation is applicable at any given time—and to which organizations they are applicable—over the course of the operation. Whether applicable statutes expand authorities or impose limitations, these considerations are especially relevant as they factor into discussions that are focused on identifying a lead authority for inter-title cyberspace operations.

d. USA PATRIOT Act (18 USC, 50 USC, *et al*)

The USA PATRIOT Act's extensive amendments to the United States Code[210] make it arguably the most controversial legislation of the 21st century. Originally passed in the wake of the 9/11 terrorist attacks, Congress intended the sweeping legislative changes to enable quick responses for deterring any near-term terrorist attacks and for investigating and prosecuting those responsible for the 9/11 attacks. The imminent nature of the threat does not appear at first to have been a long-term consideration. This is presumed based on the temporary nature of most of the provisions within the USA PATRIOT Act—referred to as sunset provisions. Many of the more controversial measures within the Act were intended to sunset after little more than four years, but, all told, have been extended nearly 14 years beyond their original life expectancy.[211] Many of the measures have since been made permanent while only a handful have been subjected to congressional repeal. As a point of commentary, this progression appears to be part of a greater realization that the new legal framework must respond to the likelihood that the threat of terrorism may be a permanent fixture across the global arena.

---

[210] The following ten titles were amended by the USA PATRIOT Act: 8 USC, 12 USC, 15 USC, 18 USC, 20 USC, 31 USC, 42 USC, 47 USC, 49 USC, and 50 USC.

[211] *See* generally "Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA FREEDOM) Act of 2015," Pub. L. 114–23 (June 2, 2015). The expiration of USA PATRIOT Act measures on June 1, 2015 amounts to little more than legislative politics. In effect, the USA FREEDOM Act, which was signed into law the very next day on June 2, 2015, restored every relevant measure from its predecessor with major revisions to only one section (50 USC § 1861) that prevents bulk data collection associated with accessing "business records for foreign intelligence and international terrorism investigations."

A closer examination shows that the Act's primary objective was improved capability against terrorism, which is obvious by the title and made apparent by the introduction of numerous sections of the USC that specifically address terrorism.[212] One recurring criticism, however, involves the definition of terrorist activity, which was expanded to include the vague term, "domestic terrorism."[213] While seemingly straightforward, there are many more innocuous activities that can easily meet the criteria for this definition—for example, a protest gone-awry. This ambiguity favors an increase in the number and type of instances under which the federal government can conduct investigations and possibly achieve convictions.[214] This concern is exacerbated further by parallel measures that broaden the authorities for the type of communications that the federal government can intercept and the conditions under which they can be intercepted and stored. Many of these provisions relate to the prevention, detection, and prosecution of personnel or institutions with international ties to money laundering associated with financing terrorist groups.[215] Other measures, however are not so high profile, and can effectively lower the threshold for

[212] 8 USC §1226A, 15 USC §1681v, 18 USC §§ 175b,1992,2339,2712, 31 USC § 5318A, 50 USC § 403-5b (now § 3143), and 51 USC § 5103a. Further, 18 USC §§ 2339,2339A, 2339B,2339C,2339D relate to harboring, supporting, financing, and receiving training from terrorists and terrorist organizations.

[213] 18 USC § 2331(5). "The term "domestic terrorism" means activities that— (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended— (i) to intimidate or coerce a civilian population;(ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States.

[214] *See* generally, United States Secret Service, "CYBER CRIME: The U.S. Secret Service Partners with State, Local and International Law Enforcement to Pursue the World's Most Wanted Cyber Criminals," trifold handout at Massachusetts Collectors and Treasurers Association Virtual Conference, 2015 (Washington DC: DHS, 2015) http://mcta.virtualtownhall.net/pages/MCTA_Presentations/2015-06/USSS%20Cyber%20Programs%20phamphlet%203-13-15.pdf. Pamphlet boasts that "since 2001, the USSS has arrested over 10,000 suspects for cyber crime related violations, and prevented over $13 billion in potential losses to victims. Finally, the USSS has continued its long-standing tradition of excellent partnerships with U.S. Attorneys' Offices, achieving a high conviction rate of **99.4%** for all cases that went to trial" (author's emphasis).

[215] Amended 18 USC §§ 981,1956(c)(7)(D), *et seq*.

conviction with many violations of federal law showing no punitive difference between conspiracy to commit the act and committing the act itself.[216]

Greater fidelity, however, is gradually being achieved in this area. The definition so far remains unchanged, but critical amendments in 2006 to sections like "Civil Forfeiture"[217] no longer address domestic terrorism as a generality. Instead, this revised section references a list of specific terrorist acts that must be engaged in before a person is made subject to the punitive measures of that statute.[218] Even with these amendments, significant search and seizure concerns exist and, more pertinent to ensuing discussion, areas like cyberspace remain open to broad interpretation. This is especially evident in those sections that relate terrorist activities to computers.[219]

This area of crimes as they relate to networks and information technology will occupy the remainder of USA PATRIOT Act discussions here. In contrast to legislative discussions thus far, in which significant abstractions must be overcome in order to establish relevance within the context of inter-title cyberspace operations, the trio of Acts that follow—FISA, ECPA, and CFAA—directly address and more closely relate to the cyberspace domain. CISA shares many of the same concerns with these preceding three, but will be discussed in its own section since it is well removed—by more than a decade—from the initial intentions of the USA PATRIOT Act.

---

[216] 18 USC §§ 81,930, *et seq*.

[217] 18 USC § 981

[218] Relevant sections still maintain broad definitions for domestic terrorism in their statutory application (c.f., 11 USC § 101, 18 USC §§ 226,1001,1028,1505, 18 USC App Fed R Crim P Rule 41, 26 USC § 6103, 28 USC §§ 530C,599A,994, 42 USC §§ 300d-71,3714a, 50 USC §§ 2314,3056).

[219] In accordance with 18 USC § 1030(a)(1), hackers who unlawfully access federal computers (as well as anyone supporting them pursuant to 18 USC §§ 2339, *et seq.*) can be charged with the federal crime of terrorism. Additionally, in accordance with 18 USC § 1030(a)(5)(A), anyone responsible for the creation of a virus that damages another computer (as well as anyone supporting them, pursuant to 18 USC §§ 2339, *et seq.*) federal crime of terrorism. Additional provisions covering violations resulting in damage as defined in 18 USC § 1030(c)(4)(A)(i)(II) through (VI) can result in federal terrorism charges. Note: The federal crime of terrorism is defined in 18 USC § 2332b(g)(5).

FISA (50 USC §§ 1801, et seq.): The attacks of 9/11 have been previously cited—over several instances—as forcing a significant shift in policy and legislation that has subsequently led to both planned and unforeseen changes that affect U.S. operations in cyberspace. In most regards, these changes led to looser restriction and greater leeway for agencies in determining how to best approach foreign and domestic threats to national security. While by no means reversing this trend, the Snowden media leaks slowed these processes and made previously hidden aspects of the federal government the subject of public scrutiny. There was arguably no legislation more affected by this than FISA, which had congressional lawmakers scramble to propose a FISA Improvements Act[220] less than six months after Edward Snowden became an internationally recognized name. This all happened despite the fact that even though the SSCI found "instances of inadvertent non-compliance;" the committee maintained that over the life of the bulk data collection program,[221] they had "not identified a single case in which a government official engaged in a willful effort to circumvent

[220] U.S. Congress, Senate, Select Committee on Intelligence, *FISA Improvements Act of 2013*, 113th Cong., 1st sess., 2013, S. 1631, https://www.congress.gov/113/bills/s1631/BILLS-113s1631pcs.pdf. The intention of this bill was, more or less, achieved by the sunset provisions of the USA PATRIOT Act (Pub. L. 107-56 s. 215) and subsequent amendments as contained in the USA FREEDOM Act of 2015. U.S. Congress, House, Committees on Oversight and Government Reform, *et al.*, *A Bill to Repeal the Cybersecurity Act of 2015*, 114th Cong., 2nd sess., 2016, H.R. 4350, https://www.congress.gov/114/bills/hr4350/BILLS-114hr4350ih.pdf

[221] *See* ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT. Pub. L. 107-56, s. 215. *See* also *Barack Hussein Obama, et al., appellants v. Larry Elliott Klayman, et al., appellees*, in Court Decision of U.S.D.C. D.C.C., No. 14-5004 (2015), https://www.cadc.uscourts.gov/internet/opinions.nsf/ED64DC482F286F1785257EAF004F71E8/$file/14-5004-1570210.pdf. The court decision vacated a preliminary injunction entered by the District of Columbia Circuit Court after determining that there were no additional restrictions imposed by the 180-day extension afforded by s. 215 of the USA PATRIOT Act following its expiration (*cf.* Klayman v. Obama, D.D.C., 13-CV-851, ECF No. 77 (2014)). This ruling effectively extended the bulk data collection program out to December 1, 2015. The extensions—provided for in the USA FREEDOM Act—were intended to facilitate a progressive draw-down in dependency on this type of collection. *See* also Ellen Nakashima, "NSA's Bulk Collection of Americans' Phone Records Ends Sunday," *Washington Post*, November 27, 2015, https://www.washingtonpost.com/ world/national-security/nsas-bulk-collection-of-americans-phone-records-ends-sunday/2015/11/27/75dc62e2-9546-11e5-a2d6-f57908580b1f_story.html.

or violate Section 215 in the conduct of the bulk telephone metadata program."[222]

These increasingly frequent federal responses were a clear indication of just how significantly FISA had changed since the original was passed in 1978.[223] Furthermore, the variation of responses showed that following this new statutory framework for electronic surveillance was evidently more difficult than originally anticipated with the additional contexts of counterterrorism, homeland security, and cybersecurity that have characterized the post-9/11 United States. It was in an attempt to address these contexts that the framework for FISA was significantly amended under the USA PATRIOT Act for the purpose of enabling counterterrorism efforts and assuring homeland security. The most significant increase in capability and authorities, however, did not come until the Protect America Act (PAA) of 2007[224] was signed into law. This act—effectively reauthorized by the FISA Amendments Act of 2008 (FAA)[225] and re-provisioned under the USA FREEDOM Act of 2015[226]—modernized FISA to enable intelligence agencies to support national interests in light of rapid technological advances.

As FISA has been more frequently applied to cyberspace operations, an item of increasing importance is an understanding of how electronic surveillance is defined by this Act, since it differs significantly from the interception of electronic communications under ECPA statutes. 50 USC § 1801(f) defines "electronic surveillance" as:

> (1) *the acquisition* by [any surveillance device] *of the contents of any* wire or radio *communication* sent by or intended to be received

---

[222] *See* BACKGROUND AND NEED FOR LEGISLATION. Senate, *FISA Improvements Act of 2013*, 1–4.

[223] *See* generally *Wikipedia*, s.v. "Foreign Intelligence Surveillance Act," last modified February 28, 2016, https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act.

[224] Pub. L. 110-55

[225] Pub. L. 110-261

[226] Pub. L. 114-23

> by a particular, *known United States person* who is *in the United States*[227] (emphasis mine).
>
> (2) *the acquisition* by [any surveillance device] *of the contents of any* wire *communication* to or from a person *in the United States, without* the *consent* of any party thereto[228] (emphasis mine).
>
> (3) *the intentional acquisition* by [any surveillance device] *of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy* and a warrant would be required for law enforcement purposes [if sender and all recipients are in the United States] (emphasis mine).
>
> (4) *the installation or use of [any surveillance device] in the United States for monitoring to acquire information*, other than from a wire or radio communication, under circumstances *in which a person has a reasonable expectation of privacy* and a warrant would be required for law enforcement purposes (emphasis mine).

The emphasis in these relevant statutes is intended to demonstrate the broad nature of these definitions, which has the capacity to encompass every electronic communication that passes within the grasp of the IC—within the jurisdiction of foreign intelligence and other exceptions. However, while the definition remains broad, the restrictions against using FISA are plentiful. In the first instance, facts must be submitted to the Attorney General that give probable cause to believe that "the target of the electronic surveillance is a foreign power or the agent of a foreign power."[229] This stipulation is further restricted by forcing the exclusion of all evidence that may be protected under the First Amendment. In other words, the federal government is not allowed to surveil someone based on expressions of free speech as protected under First Amendment constitutional rights.

---

[227] 50 USC § 1801(f)(1) further stipulates "if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."

[228] 50 USC § 1801(f)(2) further stipulates "if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18."

[229] 50 USC § 1805(a)

FISA additionally allows for the employment of pen register and trap and trace surveillance devices. Pen register devices are used to capture destination information for outgoing communications. Trap and trace devices capture the information coming to the source (trap) and then subsequently enumerate information about its originating point as well as the communication path (trace). The ECPA—discussed later—employs these for domestic investigations, while FISA investigations are for the purpose of obtaining "foreign intelligence information[230] or to "protect against international terrorism or clandestine intelligence activities."[231]

This narrow area aside, investigations approved under FISA are merely required to have foreign intelligence as "a significant purpose of the surveillance."[232] This may appear to broaden the scope for electronic surveillance, but when issuing a court order under FISA, approval is dependent on the intention of the surveillance being for the purpose of foreign intelligence.[233] That is not to say that relevant and legally obtainable information gathered over the course of the surveillance must be discarded. Instead, it simply requires that any FISA-approved surveillance be for the primary purpose of foreign intelligence.[234] For cyberspace operations, FISA allows for inter-title cooperation,[235] but its narrow focus likely requires that FISA considerations be used in a complimentary role for operations with a broader scope.

Business records are also subject to FISA inquiry.[236] Interestingly, however, the FBI is the only agency permitted to submit applications for this

[230] Pursuant to 50 USC § 1842(a)(1), foreign intelligence information for pen register and trap and trace devices are not authorized to concern a United States person.

[231] 50 USC § 1842(a)(1)

[232] 50 USC § 1804(a)(6)(B) relating to electronic surveillance, 50 USC § 1823(a)(6)(B) relating to physical searches, 50 USC § 1881a(g)(2)(A)(v),1881b(1)F)(ii),1881c(b)(5)(B) pertaining to certain persons outside the United States.

[233] As described in 50 USC § 1801(e) pertaining to electronic surveillance.

[234] In accordance with the definition set forth in 50 USC § 1842(a)(1).

[235] In accordance with presidential policy (c.f., EO 12139, s. 1-103).

[236] 50 USC § 1801

information. This does not necessarily restrict other members of the IC from accessing this information or making requests for it, but simply requires that all requests be ultimately vetted and submitted by the Director of the FBI.[237]

One final consideration is of particular importance and concerns the Foreign Intelligence Surveillance Court's (FISC) burden of proof for refusing an erroneous federal application. After a FISA application has been appropriately vetted and determined to align with definitions and purposes, the FISC is then required to issue a court order so long as the application and its supporting information is "not clearly erroneous."[238] In the minds of some, this has the appearance of spuriously favoring intelligence agencies, but this concern, however appropriate, is not a malformation of jurisprudence. In light of the extensively detailed information requirements and the extensive vetting process that precedes application submissions for court orders,[239] the burden of proof, which rests on the FISA Courts, assures a normative response once federal mandates have been met. Those who are concerned with the structure of this process would likely be astonished at conditions under which electronic surveillance may be authorized without a court order.[240] Even in these cases, however, the Attorney General must certify that there "is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party."[241]

The point here—indeed throughout—is not to uncover discomforts with the current legal process, even if they pose relevant questions to executive

---

[237] Or, as stipulated in 50 USC § 1801(a), applications may also be submitted by "a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge)."

[238] Pursuant to 50 USC § 1805(a)(4).

[239] Pursuant to 50 USC § 1804.

[240] Pursuant to 50 USC § 1802.

[241] 50 USC § 1802(a)(1)(B). *See* OTHER POSSIBLE EFFECTS OF NEW SECTIONS 105A, 105B, and 105C. Elizabeth B. Bazan, *The Foreign Intelligence Surveillance Act: Overview and Modifications* (New York: Nova Science, 2008), 11–14. Though her exceptional work on FISA in now slightly dated in light of FAA amendments, Bazan maintains many relevant positions on other possibly objectionable actions that have the potential to allow for circumventing the oversight of the FISC.

procedure. Instead, these lines of examination are intended to show that, no matter how contentious, the extensive processes that are currently in place provide the necessary oversight and compliance to enable expanded cooperative efforts between agencies that may traditionally be more familiar with operating along narrower lines of authorities. This oversight and compliance is one of the key discussion points and, in the specific case of FISA, it is clear that it extends well beyond the FISA Courts. The Permanent Select Committee on Intelligence of the House of Representatives (HPSCI) and the Select Committee on Intelligence of the Senate also have extensive oversight to ensure compliance with all aspects of the FISA program,[242] and legislation affords aggrieved parties to appeal decisions[243] or to retrospectively recoup damages associated with FISA violations.

ECPA (18 USC § 2510, et seq.)*:*[244] The ECPA was significantly modified by the USA PATRIOT Act to provide greater clarity to jurisdictions as they applied to new and emerging technologies. Behaviors and methods associated

---

[242] Pursuant to 50 USC §§ 1807,1808 relating to electronic surveillance; 50 USC § 1826 relating to physical searches; 50 USC § 1846 relating to pen registers and trap and trace devices; 50 USC § 1862 relating to business records; 50 USC §§ 1871, *et seq.* relating to program oversight; 50 USC § 1881f relating to additional procedures.

[243] *See* generally "Statement by the ODNI and the U.S. DOJ on the Declassification of Documents Related to the Protect America Act Litigation," Office of the Director of National Intelligence press release, September 11, 2014, accessed January 8, 2016, http://www.dni.gov/index.php/newsroom/ press-releases/198-press-releases-2014/1109-statement-by-the-office-of-the-director-of-national-intelligence-and-the-u-s-department-of-justice-on-the-declassification-of-documents-related-to-the-protect-america-act-litigation?tmpl=component&format=pdf. Internet company, Yahoo!, "opposed the U.S. Government's motion to compel compliance with [FISA] directives primarily on the ground that the directives violated the Fourth Amendment rights of its customers. On April 25, 2008, following extensive briefing by the parties, the FISC held that the directives were lawful and ordered Yahoo! to comply."

[244] *See* generally Donald P. Delaney, Dorothy E. Denning, John Kaye and Alan R. McDonald, *Wiretap Laws and Procedures: What Happens When the U.S. Government Taps a Line*, white paper distributed by D.E. Denning, Professor and Chair Computer Science Department at Georgetown University (Washington DC: Georgetown University, 1993), http://faculty.nps.edu/dedennin/ publications/WiretapLawsProcedures.txt. This part of ECPA was actually an amendment of the Omnibus Crime Control and Safe Streets Act of 1968, which contained a wiretap statute that already covered wire and oral communications. The ECPA added electronic communications so as to clarify that electronic communications were also protected from access. *See* also DEFINITIONS. 47 USC § 1001. Definitions altered by the USA PATRIOT Act of 2001 provided significant increases in authority for the FBI—most especially in the area of counterterrorism.

with using these technologies were as influential in legislation and subsequent legal opinions as the technology itself. The amended version of the ECPA protects *all wire, oral, and electronic communications during t*heir inception, transmission, or storage. ECPA provides protections for private chat, email, and electronically stored data, and also protects telephone conversations delivered through both the Public Switched Telephone Network (PTSN) and Voice over IP (VoIP).

The ECPA has three titles. Title I, often referred to as the Wiretap Act,[245] prohibits the intentional attempted or actual interception of any "wire, oral, or electronic communication" or the intentional disclosure of such information if it was obtained in violation of federal law.[246] It also prevents all subsequent information from being used in court if its procurement was federally prohibited.[247] Though the Wiretap Act is contained in Title 18, it is by no means isolated from other title authorities. For example, this section of the ECPA makes provision for collection that is for the purposes of foreign intelligence authorized under FISA.[248]

There are three significant exceptions to the Wiretap Act that affect cyberspace operations. The first allows "for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic

[245] 18 USC §§ 2510–2522

[246] Pursuant to 18 USC § 2511.

[247] Pursuant to 18 USC § 2515.

[248] 18 USC sec 2511(2)(a)(iii))

surveillance."[249] The second is a "provider" exception that allows service providers to supply customer records and monitor calls or record information when directed by law enforcement officers operating under a valid court order,[250] in the course of normal service provision,[251] for maintenance related purposes,[252] or in the protection of their property.[253] The third exception is applicable "where one of the parties to the communication has given prior consent to such interception."[254]

Title II[255] of the ECPA is referred to as the Stored Communications Act (SCA)[256] and is focused on providing privacy protections against the unauthorized viewing of electronic files and associated records that are stored by service providers. These provisions broadly cover personal identifiers like subscriber and billing information as well as any applicable IP ranges. The structure of the SCA is unique because it varies the degree to which privacy

[249] Pursuant to 18 USC § 2511(2)(e) "as defined in section 101 of the Foreign Intelligence Surveillance Act (FISA) of 1978." Though patently obvious, the "normal course of law enforcement" is subject to the rigorous statutes governing federal investigations and criminal procedure. *See* SPECIFIC PROVISIONS. "Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510–22," DOJ Bureau of Justice Assistance, DHS Office for Civil Rights and Civil Liberties, DHS Privacy Office, last modified July 30, 2013, https://it.ojp.gov/privacyliberty/authorities/statutes/1285. "[ECPA] provides procedures for Federal, State, and other government officers to obtain judicial authorization for intercepting such communications, and regulates the use and disclosure of information obtained through authorized wiretapping. 18 U.S.C. § 2516–18. A judge may issue a warrant authorizing interception of communications for up to 30 days upon a showing of probable cause that the interception will reveal evidence that an individual is committing, has committed, or is about to commit a "particular offense" listed in § 2516. 18 U.S.C. § 2518."

[250] Pursuant to 18 USC § 2511(2)(a)(ii)

[251] Pursuant to 18 USC §§ 2511(2)(a)(i),2702(b)(5). This can include random monitoring that is intended to report the health of the system or ensure network optimization.

[252] Pursuant to 18 USC § 2511(2)(a)(i)

[253] Ibid. One example of service providers using this property protection clause is to monitor or prevent the use of their network from unauthorized users.

[254] Pursuant to 18 USC § 2511(2)(d)

[255] 18 USC §§ 2701–2712

[256] *See* NOTE 1. Computer Crime and Intellectual Property Section (CCIPS), *Searching and Seizing Computers and Obtaining Electronic Evidence In Criminal Investigations*, (Washington DC: Office of Legal Education, 2009), 115, http://www.justice.gov/sites/default/files/ criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf. "Although 18 U.S.C. § 2701–2712 is referred to as the "Stored Communications Act" here and elsewhere, the phrase "Stored Communications Act" appears nowhere in the language of the statute"

concerns apply based on the type of information being stored.[257] For example, from the perspective of ECPA, the contents of stored emails are of significantly higher concern than information associated with the subscriber. A consequence of this is the variety of legal processes that must be followed based on the nature of the desired content, to include a subpoena, special court order, or even a search warrant. Of even greater concern are the provisions that may or may not even require the subscriber to be notified of certain federal actions. The few exceptions that permit access to stored communications appear to favor the subscriber by offering "varying degrees of legal protection depending on the perceived importance of the privacy interest involved."[258]

The third and final section[259] of the ECPA is closely related to the first and the pair of them are primarily responsible for enabling real-time electronic surveillance as part of ongoing federal criminal investigations.[260] This section outlines authorities and procedures for obtaining court orders for the employment of the pen register and trap and trace surveillance devices covered previously under FISA discussions. Since no communication content is captured by these devices, they are often required to be used in conjunction with provisions under the Wiretap Act in order to gain insight into the exact nature of the electronic communication.

CFAA (18 USC § 1030): The CFAA has been amended numerous times since it was first passed in 1986, including its own inception, which was really an amendment to the provisions of the computer fraud law that was incorporated

---

[257] *See* APPENDIX B – Quick Reference Guide for the Stored Communications Act.

[258] Ibid., 115.

[259] 18 USC §§ 3121–3127

[260] *See* ELECTRONIC SURVEILLANCE IN COMMUNICATIONS NETWORKS. CCIPS, *Searching and Seizing Computers and Obtaining Electronic Evidence In Criminal Investigations*, 151–90.

into legislation from 1984.[261] In January of 2015, President Barak Obama proposed legislation[262] that would more effectively combat cybercrime through expanded authorities to both the CFAA and the Racketeer Influenced and Corrupt Organizations (RICO) Act.[263] This announcement met with notable public criticism as proposed expansions to authorities were perceived as diversion from the original intent of the CFAA.[264]

Attempts to revise and clarify laws based on changes to the cyberspace landscape are a normal course for most applicable legislation. Though difficulties exist in applying rapidly evolving processes and methodologies to the glacial pace of legislation, the DOJ in particular has made significant inroads through extensive policies and procedure manuals—most especially those that address federal laws as they relate to computer crimes.[265] These manuals specifically concentrate on crimes that target information technology or are enabled by it. For

---

[261] The computer fraud law created 18 USC § 1030 under the Comprehensive Crime Control Act of 1984 (Pub. L. 98-473). The CFAA that amended it has since received minor amendments in 1988 (Pub. L. 100-690), 1989 (Pub. L. 101-73), 1990 (Pub. L. 101-647), 1994 (Pub. L. 102-322), and 2002 (Pub. L. 107–273 and 107–296) with major revisions in 1996 (Pub. L. 104–294), under the USA PATRIOT Act in 2001 (Pub. L. 107–56), and in 2008 (Pub. L. 110–326).

[262] *See* "SECURING CYBERSPACE - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts," Office of the Press Secretary press release, January 13, 2015, accessed August 11, 2015, https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

[263] Pub. L. 91-452 leading to the creation of 18 USC §§ 1961, *et seq*. The Act was a response to growing criminal influence by Organized Crime syndicates. *Cf.* RICO'S LEGISLATIVE HISTORY. Organized Crime and Racketeering Section, *Criminal RICO: 18 U.S.C. §§ 1961–1968, A Manual for Federal Prosecutors*, 5th ed. (Washington DC: DOJ, 2009), 3–16, http://www.justice.gov/sites/default/files/usam/legacy/2014/10/17/rico.pdf.

[264] *See* generally "Lofgren, Wyden, Paul Introduce Bipartisan, Bicameral Aaron's Law to Reform Computer Fraud and Abuse Act," press release by Peter Whippy, April 21, 2015, accessed August 11, 2015, https://lofgren.house.gov/news/documentsingle.aspx?DocumentID=397911. *See* also Mark Jaycox, "Broad Coalition of Groups Oppose CFAA Amendment to CISA Surveillance Bill," *Electronic Frontier Foundation*, October 3, 2015, https://www.eff.org/deeplinks/2015/10/bipartisan-groups-oppose-cfaa-amendment-cisa-surveillance-bill.

[265] *See* CCIPS, *supra* note 260. *See* also PREFACE AND ACKNOWLEDGEMENTS. Computer Crime and Intellectual Property Section, *Prosecuting Computer Crimes*, 2nd ed. (Washington DC: Office of Legal Education, 2015), v-vi, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf. The CFAA is limited in that it cannot cover every issue, like "state [laws] [nor] […] every type of crime related to computers, such as child pornography or phishing." *See* APPENDIX A. *Id.* at 149–55. Even with these limitations, however, there are still considerable provisions under Title 18 for procedures that enables prevention of cybercrime under applicable sections (i.e., 18 USC §§ 875, 1343, 1951, 2251, *et seq.*).

the FBI, it is significant to note that computer crime is synonymous with cybercrime and network crime. Examples of cybercrime that are specifically envisioned by this Act include those that are "interstate in nature" and include methods like DOS, DDOS, computer and network intrusions, and the implanting of malicious code.[266] These manuals are unable to address every concern, but instead provide guidelines for clarifying investigative procedure as it relates to the nature of the cybercrime.

The overall intent of the law and subsequent amendments has been to equate criminal conduct with any activity that victimizes computers and computer networks. There are seven distinct types of criminal activity that are considered violations of the CFAA (Fig. 1). Shocking as it may be, when viewed as a whole, these seven criminal violations effectively cover ever computer, and computer device in the world. Even though the term "protected computer" portends to address only computers owned by the government, and those relevant to national security and the economy, in practice it has constituted every computer that is connected to the Internet.[267]

---

[266] Ibid.

[267] *See* PROTECTED COMPUTER. Corey Varma, "What is the Computer Fraud and Abuse Act (CFAA)?," *Cyberspace Law, Information Technology And Privacy Law*, January 3, 2015 http://www.coreyvarma.com/2015/01/what-is-the-computer-fraud-and-abuse-act-cfaa/#protected_computer. "In *US v. Trotter*, the Defendant argued that his former employer's computer network was not a 'protected computer' as set forth in 18 U.S.C. § 1030(e)(2)(B). The 8th Circuit rejected this claim and affirmed the Defendant's conviction because the Defendant admitted, at a plea hearing, that his former employer's network was connected to the Internet. The Court used this admission to determine the computer network met the statutory definition of a 'protected computer.'"

Figure 1. Summary of CFAA Penalties

Offense	Section	Sentence*
Obtaining National Security Information	(a)(1)	10 (20) years
Accessing a Computer and Obtaining Information	(a)(2)	1 or 5 (10)
Trespassing in a Government Computer	(a)(3)	1 (10)
Accessing a Computer to Defraud & Obtain Value	(a)(4)	5 (10)
Intentionally Damaging by Knowing Transmission	(a)(5)(A)	1 or 10 (20)
Recklessly Damaging by Intentional Access	(a)(5)(B)	1 or 5 (20)
Negligently Causing Damage & Loss by Intentional Access	(a)(5)(C)	1 (10)
Trafficking in Passwords	(a)(6)	1 (10)
Extortion Involving Computers	(a)(7)	5 (10)

* The maximum prison sentences for second convictions are noted in parentheses.

Source: Computer Crime and Intellectual Property Section, *Prosecuting Computer Crimes*, 2nd ed. (Washington DC: Office of Legal Education, 2015), 3.

Upon initial examination, the law appears designed to target two types of perpetrators through two key distinctions. This first concerns those who access a computer based on the sole condition that it is done "without authorization."[268] The second includes an additional provision that the perpetrator "exceeds authorized access."[269] There is also a third provision that broadly covers extortion that is coerced through threats to commit these preceding violations.[270] In the first instance, the term "without authorization" appears to be plainly obvious because it is not included in the section under definitions. In the second instance, however, the term "exceeds authorized access" is defined as an instance where a perpetrator has authorized "access to a computer" and uses that access "to obtain or alter information in the computer that [he] is not entitled [to]."[271] From this, the two key distinctions appear to be based loosely on crimes perpetrated

[268] Relevant sections include 18 U.S.C. §§ 1030(a)(3),1030(a)(5),1030(a)(6).

[269] Relevant sections include *id.* at §§ 1030(a)(1),1030(a)(2),1030(a)(4).

[270] 18 U.S.C. § 1030(a)(7).

[271] 18 U.S.C. § 1030(e)(6).

by insider threats and those perpetrated by outsider threats.[272] According to the FBI's manual on Prosecuting Computer Crimes,

> The legislative history of the CFAA reflects an expectation that persons who "exceed authorized access" will be insiders (e.g., employees using a victim's corporate computer network), while persons who access computers "without authorization" will typically be outsiders (e.g., hackers).[273]

Those threats that deal with national security entail threats from both insiders and outsiders, while trespassing, computer damage, and password stealing are seen as almost strictly involving outsiders. The difference between insiders and outsiders is significant when introducing the idea of inter-title cooperation, most especially as it involves the military. Since special emergency circumstances are unlikely—though not impossible—to justify the use of the military, threats that are perpetrated solely by domestic insiders would likely exclude military involvement except as authorized under relevant intelligence sharing provisions.[274]

For investigations involving outsiders who are not U.S. persons or are U.S. persons who may be investigated pursuant to applicable sections of FISA, inter-title cooperation may be a legally viable avenue and fiscally desirable avenue. Involvement from the armed forces, DHS, the NSA, the Coast Guard, or any number of agencies may be desirable so long as those agencies are

---

[272] *See* CYBERCRIME LAW: A UNITED STATES PERSPECTIVE. Susan W. Brenner, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd ed., ed. Eoghan Casey (New York: Academic Press, 2011), 85–122. The threat from an involves primarily insider activity concern threats that are introduced by a trusted user with authorized access to a computer. Though this includes unknowing individuals, 18 U.S.C. § 1030(e)(6) makes clear that the perpetrator must 'knowingly' or 'intentionally' commit the alleged offenses. Outsider threats, by contrast, are perpetrated by individuals who have "no authorization to access the computer or computer system."

[273] CCIPS, *Prosecuting Computer Crimes*, 5-6. "*See* S. Rep. No. 99-432, at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479 (discussing section 1030(a)(5), 'insiders, who are authorized to access a computer, face criminal liability only if they intend to cause damage to the computer, not for recklessly or negligently causing damage. By contrast, outside intruders who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass.'); S. Rep. No. 104-357, at 11 (1996), *available at* 1996 WL 492169; *United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007) (discussing legislative history)."

[274] *See supra* note 197.

equipped with some unique capability to aid in prosecution or are not degraded in their own primary mission areas by providing assistance. This is especially true for instances involving violations that threaten national security—a topic for which there is significant overlap between countless federal agencies.[275] These considerations do not appear to be recent revelations for legislators who apparently recognize the overlap and clarify that the CFAA is not intended to "prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency […] or of an intelligence agency."

There are certainly more considerations than those listed previously, like ensuring compliance and reporting with relevant sections on oversight,[276] but necessary training and compliance measures are not beyond the capability of a lead agency to coordinate and implement. For cases of CFAA violations, the FBI is designated as the "primary authority to investigate offenses" to National Security Information[277] "involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations."[278] Specifically, any pending investigation or indictment under 18 U.S.C. § 1030(a)(1) "requires the prior approval of the National Security Division of the Department of Justice, through the Counterespionage Section."[279] As stated earlier, however, the delineation of lead authorities and coordinating bodies does not preclude the involvement of other entities.

---

[275] *See* generally "National Security Council," U.S. White House, accessed March 11, 2016, https://www.whitehouse.gov/administration/eop/nsc. "The NSC is chaired by the President. Its regular attendees [are] […] the *Secretary of State*, the *Secretary of the Treasury*, the *Secretary of Defense*, and the Assistant to the President for National Security Affairs. The *Chairman of the Joint Chiefs of Staff* is the statutory military advisor to the Council, and the *Director of National Intelligence* is the intelligence advisor. […] The *Attorney General* and […] [the] *heads of other executive departments and agencies*, as well as other senior officials, are invited to attend meetings of the NSC when appropriate" (emphasis mine).

[276] 18 USC § 1030(h) *et al*.

[277] Pursuant to 18 USC § 1030(a)(1).

[278] 18 USC § 1030(d)

[279] CCIPS, "Prosecuting Computer Crimes," 12.

A good example of the potential for unifying inter-title efforts among cyberspace operators can be seen in the example of the five Chinese hackers who were charged by the DOJ in 2014 with violations of the CFAA.[280] Though there was no accompanied acknowledgement of involvement from other federal agencies or entities, the overlap that exists between the FBI and DHS in terms of critical infrastructure protection (CIP), the armed forces in the operational preparation of the environment (OPE), the NSA and CIA in their scope of foreign intelligence concerns are all examples of where title authorities would enable operations aimed at neutralizing the activities of these Chinese hackers. It is also of little concern that those aims may differ significantly between agencies and organizations. The FBI may be seeking indictment, while DHS may support operations in order to protect Critical Infrastructure stakeholders, the NSA may desire to infiltrate and enumerate foreign hacker networks, and the armed forces may seek to establish a capability against any of the observed cyberspace methodologies. These intentions matter little so long as they are authorized and cooperation is not explicitly prohibited.

e. CISA (Pub. L. 114-113, Div. N, Title I)

Passing as part of an omnibus bill[281] that appeared designed to address federal funding, CISA was signed into law less than two weeks before the New Year. The effects of its controversial passing remain a constant topic among

[280] *See* generally *United States of America v. Wang Dong, et al.*, in Criminal Complaint of U.S.D.C. W.D.P., No. 14-118 (2014), http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf. Of the 31 purported violations brought against the Chinese hackers identified by the DOJ, there was one count of "Conspiring to commit computer fraud and abuse" pursuant to 18 U.S.C. § 1030(b), eight counts of "Accessing (or attempting to access) a protected computer without authorization to obtain information for the purpose of commercial advantage and private financial gain" pursuant to 18 U.S.C. §§ 1030(a)(2)(C),1030(c)(2)(B)(i)-(iii), and 14 counts of "Transmitting a program, information, code, or command with the intent to cause damage to protected computers" pursuant to 18 U.S.C. §§ 1030(a)(5)(A),1030(c)(4)(B).

[281] Pub. L. 114-113.

government cybersecurity experts, legislators, and privacy advocates.[282] The arguments are many and varied, and while this paper takes no position on the ethics position in legislation, it is worth stating that the concepts of security and privacy are interdependent. The fact that the government has access to information that is protected by privacy laws does not make their accessing of it irrefutably illegal or unethical. The preceding discussions show that there are significant divergences between federal provision to national cybersecurity and private sector's provision of cybersecurity on behalf of themselves. In many ways, CISA aims to remove these obstacles and to allow time-sensitive data to be shared between industry and federal entities in ways that lead to an effective response to the ever-increasing losses experienced due to cybercrime.[283] This aim, however, does not allay fears and suspicion, nor does it solve the numerous potential conflicts that CISA poses to the legal frameworks of other laws.

Since this law primarily addresses domestic industry, pertinent concerns generally affect provisions pursuant to ECPA and CFAA as they relate to due process. As noted by numerous critics, CISA's current wording enables network monitoring, information sharing, and defensive measures to be enacted so long as they are "for a cybersecurity purpose."[284] CISA defines "cybersecurity purpose" as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[285] While this is not a complete suspension of ECPA provisions, it gives a wide berth for industry to monitor their networks and to share cybersecurity-relevant information. More than that, CISA

---

[282] *See* generally, Cory Bennett, "Cybesecurity's Winners and Losers," The Hill, December 19, 2015, http://thehill.com/policy/cybersecurity/263785-cybesecuritys-winners-and-losers. *See* also Larry Greenemeier, "A Quick Guide to the Senate's Newly Passed Cybersecurity Bill: The Basics of the Controversial Cybersecurity Information Sharing Act (CISA)," *Scientific American*, October 28, 2015, http://www.scientificamerican.com/article/a-quick-guide-to-the-senate-s-newly-passed-cybersecurity-bill.

[283] *See supra* note 50.

[284] Pub. L. 114-113, Div. N, Title I, ss. 104(a)(1),(b)(1),(c)(1)

[285] *Id.* at s. 102(4).

adds “notwithstanding” clauses to these information-sharing sections[286] that allow industry to effectively suspend provisions under ECPA’s Wiretap Act so long as their actions are conducted under cybersecurity purposes.

These provisions, while unsettling in any other setting, are not so shocking in the context of cyberspace. While the ECPA definitions may allow for monitoring on standard network nodes,[287] it has traditionally been interpreted to prevent the intentional interception of any information and further restricts the sharing of those “contents”[288] without a court order. Since the “contents” of cyberspace information are defined as “any information concerning the substance, purport, or meaning of that communication,”[289] industry cooperation on cybersecurity reporting may be easily interpreted as a violation of the Wiretap Act. Legal analyst, Susan Hennessey, notes that

> ECPA […] creates uncertainty [in the context of cybersecurity and] makes it difficult for companies to understand precisely what sort of monitoring is okay and what sort is a crime. Ambiguity in a litigation-averse culture runs contrary to a goal of responsible, proactive cybersecurity monitoring. Whether we like it or not, effective cybersecurity monitoring *likely does extend* to the contents of communications in at least some circumstances” (emphasis mine).[290]

Hennessey’s opinion is certainly not definitive, but exposes the likely intent of this Act, which is the enablement of responsible cybersecurity measures that protect private industry and Critical Infrastructure. It may appear that simply obtaining the necessary consent or incorporating this information access into service agreements is a viable replacement for CISA provisions, but the

---

[286] *Supra* note 283.

[287] *See* 18 USC §§ 2510(4),5(a)(ii). Under definitions for “intercept” and "electronic, mechanical, or other device," there may be latitude for interpreting cybersecurity devices as being “used by a provider of wire or electronic communication service in the ordinary course of its business.”

[288] 18 USC § 2510(8).

[289] Ibid.

[290] *See* THE ELECTRONIC COMMUNICATIONS PRIVACY ACT. Susan Hennessey, “The Problems CISA Solves: ECPA Reform in Disguise,” *Lawfare*, December 23, 2015 https://www.lawfareblog.com/problems-cisa-solves-ecpa-reform-disguise.

inconsistency in legal application is a cause of concern for most service providers. For example, current trends in case law have taken notice of the extensive permissions granted to corporations through their terms of service and privacy agreements. The courts have responded by holding corporations accountable to their company norms for handling information instead of permitting them to leverage the extensive service agreements that allow for broad and ambiguous exceptions to privacy protections.[291]

Despite the broad freedoms that it grants for industry sharing, for the purposes of cyberspace operations, CISA poses potential problems to inter-title cooperation. Even if industry is sharing information for cybersecurity purposes, it may be unclear whether the shared indicators have international elements or are of a purely domestic concern. In these cases, law enforcement related legal restrictions imposed by Posse Comitatus Act would become a major concern for any armed forces involvement. In spite of this, CISA very obviously enlists and necessitates cooperation between numerous departments and agencies of the federal government.[292] In order to align the handling of information with applicable statutes, the CFAA assigns the development of policy and procedure to the Attorney General (head of DOJ) and the Secretary of Homeland Security.[293] By placing the Secretary of Homeland Security as the lead agency for CISA-related information sharing provisions, CISA limits the possibilities for information abuse by making liability protection contingent on sharing with DHS.[294] The Act does, however, allow for DHS to establish an automated

---

[291] *See* THE CONSENT EXCEPTION. Ibid.

[292] Pub. L. 114-113, Div. N, Title I, ss. 103(a). "Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the *Director of National Intelligence*, the *Secretary of Homeland Security*, the *Secretary of Defense*, and the *Attorney General*, in consultation with the *heads of the appropriate Federal entities*, shall jointly develop and issue procedures to facilitate and promote [information sharing]. (emphasis mine)"

[293] *Id.* at ss. 105(a)(4), *et seq*.

[294] *See* generally, Paul Rosenzweig, "The Cybersecurity Act of 2015," *Lawfare*, December 16, 2015, https://www.lawfareblog.com/cybersecurity-act-2015.

system for sharing information with other government agencies[295] through non-DHS centers subject to executive approval and congressional notification.[296]

A particularly keen remark from Hennessy addresses the use of information that has been collected and shared pursuant to CISA.

> [This information] is limited not only by the express use provisions but also by all "otherwise applicable provisions of Federal law." Legally speaking, this provision [means that] the government has to comply with the law. Thanks for pointing that out. But it also foot stomps an important point: *Whatever the government could not do before, it cannot do now*. The government use provisions operate exclusively as a limitation, and in no way expand the government's authority. Therefore, whatever genuine civil liberties concerns CISA creates must derive from some new set of information that the government otherwise could not or would not obtain" (emphasis mine).[297]

In this case, it should be clear that the provisions of the CFAA and ECPA must remain in place and that the provisions of CISA are not intended to allow the federal government to sweep aside privacy rights[298] and access information that they are prohibited from viewing in the normal course of investigations. Instead, it appears designed to provide this information through channels that allow it to remain relevant to national cybersecurity objectives.

There is no doubt that CISA enables the federal government to access data that was previously subject to court order, but this development does not equate to a carte blanche on cyberspace information. As stated earlier, the emergence of cyberspace legislation, imperfect as it may be, is a clear indication that cyberspace threats—whether emerging or persistent—require a response

---

295 *See supra* note 291.

296 Rosenzweig, *supra* note 293.

297 *See* generally Susan Hennessey, "CISA in Context: Government Use and What Really Matters for Civil Liberties," *Lawfare*, January 14, 2016, https://www.lawfareblog.com/cisa-context-government-use-and-what-really-matters-civil-liberties.

298 *See* generally Jennifer Granick, "OmniCISA Pits DHS Against the FCC and FTC on User Privacy," *Just Security*, December 16, 2015, https://www.justsecurity.org/28386/omnicisa-pits-government-against-self-privacy. *See* also Finnegan, *supra* note 109.

that, as yet, is not effectual under current legislation.[299] This, and subsequent shifts in policy that aim to maximize inter-title cooperation, further shows that these threats are not easily addressed by any one department, agency, or private entity. The current architecture of information networks—connections, communications mediums, protocols, and network nodes—appears to require cooperation from all involved.

[299] *See* DHS, *supra* note 8.

III. ENABLING INTER-TITLE OPERATIONS

A. INTER-TITLE COOPERATION

1. The Place of Policy

Policy has played a central role in the functioning of the government since the earliest years following the founding of the United States. In the Post-Revolutionary period, the disparity in power between the government and the local militia was surprisingly small. Aside from the warship, muskets and cannon were accessible enough to deem state militias an adequate measure for national security and a reasonable deterrent against any incentive for government tyranny. Indeed, this may likely have contributed to the vague requirements levied upon the executive powers as they are outlined in Article 2 of the U.S. Constitution. This marginal inequality increased over the next 150 years in favor of the federal government—specifically, the Executive branch—but it was the advent of the nuclear bomb that induced the most dramatic and irreversible change.[300]

In the years that followed, legislative changes and legal interpretations attempted to balance the increased powers of the presidency with an appropriate level of accountability that still allowed the president to effectively execute the duties of the office. While legislation curtailing the power of the president was scarce at the outset, it eventually evolved so as to place both demands and limitations on the Executive branch in order to align executive action with the desires of Congress. Landmark legislation like the War Powers Resolution of 1973,[301] the Hughes-Ryan Amendment of 1974,[302] FISA, and the Intelligence

[300] Garry Willis, *Bomb Power: The Modern Presidency and the National Security State* (New York: Penguin Books, 2010) 1–4. For Willis, the advent of the atomic bomb in the 1940s "redefined the presidency […] [and] redefined the government as a National Security State, with an apparatus of secrecy and executive control."

[301] 50 USC §§ 1541, *et seq.*

Oversight Act of 1991[303] are all examples of the rebalancing of legislative and executive powers—not absent judiciary concurrence. In response to the aforementioned legislation, Executive Orders were issued by subsequent presidents Gerald Ford (EO 11905), Jimmy Carter (EO 12036), and Ronald Reagan (EO 12333) to reinforce this new balance, specifically as it pertained to interactions between intelligence entities—the CIA for example—and the armed forces. This is significant, because, as eluded to in previous sections, the unique response demanded from cyberspace has created similar tensions that are being resolved through available frameworks and the appropriate balance—in light of the emerging context of cyberspace[304]—continues to be refined through continual legislation and policy issuances.

The current rebalancing, as it applies to cyberspace, may easily be characterized by greater turbulence than the preceding nuclear age. Not only is the advancement of information technology proceeding at a significantly faster pace, but the barriers to ascension are substantially lower for cyberspace than they were—and presumably still are—for nuclear technology. It is not surprising, therefore, that there is also a resurgence of executive behavior that is eerily reminiscent of the Cold War era. Seedier methods for protecting national security like torture and political assassinations—banned in 1996[305] by legislation and

---

[302] *See* generally James S. Van Wagenen, "A Review of Congressional Oversight: Critics and Defenders," *CIA Center for the Study of Intelligence*, April 14, 2007, last modified June 27, 2008, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/wagenen.html. This was an "amendment to the Foreign Assistance Act of 1961 [that] addressed the question of CIA covert actions and prohibited the use of appropriated funds for their conduct unless and until the President 'finds' that each such operation is important to the national security and submits this Finding to the appropriate Congressional committees--a total of six committees."

[303] Pub. L. 102-88. Title VI of this Act provided Congress with increased oversight of intelligence activities and specifically "bars the President from authorizing the conduct of covert actions" as outlined in the Act and further mandates congressional notification of any necessary covert activities "before the covert action is initiated."

[304] There are inevitably dependencies between this emerging context—profoundly impacted by terrorism and networked technology—and the prominent rise of national security concerns over the latter half of the 20th century. In this emerging context, it is important to realize that the nature and accessibility of cyberspace dramatically shrinks the power disparity, but in no way removes previous technological advancements.

[305] Pub. L. 103-236

1976 by executive order,[306] respectively—became acceptable tenets in early counterterrorism efforts.[307] These inclinations, combined with a generally acknowledged need for total secrecy in active cyberspace operations, makes it of even greater importance that federal policies clearly discern the intent, extent, and provisions of the law.

Federal policies not only provide a framework for effectively and legally accomplishing the goals of national security and furthering U.S. national interests, but they also work to mitigate risk and manage decision making.[308] The relationship between policy and legislation is often misunderstood and the restrictions imposed by policy and procedures are often confused for restrictions imposed by the law. For example, the laws concerning FISA may state that the federal government must apply for a court order with the minimum information outlined in the statute, but the policy imposed by the president could place greater demands on those applications or even require that the information be further validated through a specific source or method. Furthermore, each agency can set up organizational policies that restrict the federal employees who may be responsible for initial vetting of applications before they are officially submitted to the Attorney General or forwarded on to the FISC.

This murky environment is inundated with memoranda that are provisioned by various echelons of organizational policy that is in turn contingent

---

[306] EO 11905

[307] Regarding TORTURE: The federal prohibition against torture (codified under 18 USC §§ 2340, *et seq.*) has been made significantly more complex by early 21st century domestic legislation and policies that redefined previously banned procedures as "enhanced interrogation techniques." *Cf.* "USA and Torture: A History of Hypocrisy," Human Rights Watch, December 9, accessed March 11, 2016, https://www.hrw.org/news/2014/12/09/usa-and-torture-history-hypocrisy. *See* also Stephen G. Bradbury, "RE: Application of 18 U.S.C. §§ 2340–2340A to Certain Techniques That May Be Used in the Interrogation of a High Value al Qaeda Detainee," memorandum for John A. Rizzo, Senior Deputy General Counsel, Central Intelligence Agency, May 10, 2005, https://www.justice.gov/sites/default/files/olc/legacy/2013/10/21/memo-bradbury2005-3.pdf. *See* also *supra* note 130. Regarding ASSASSINATIONS: *See* A THUMBNAIL SKETCH OF THE ORIGINS OF THE SHADOW WAR. Chesney, "Beyond The Battlefield, Beyond Al Qaeda: The Destabilizing Legal Architecture of Counterterrorism," 205-06. *Cf.* Zenko, *supra* note 138.

[308] *See* generally, Todd F. Gaziano, "The Use and Abuse of Executive Orders and Other Presidential Directives," *Texas Review of Law & Politics* 5, no. 2 (Spring 2001): 267–97.

upon overarching legal and procedural policy that is ultimately subject to legislation. Ideally, this would make the lowest levels subject to the most restrictive aspects of policy, but this expectation is rarely the case when policies from one organization become entangled with the policies from another—as is often the case for inter-title operations. A classic example is found in the diverse classification policies that characterize various agencies within the federal government.[309] The complex and diverse classification interpretations that exist between disparate government entities make information sharing an extremely difficult and complex endeavor. Prior to the information sharing mandates of 2001, this is one of the reasons that agencies avoided planning and executing operations outside of their own organization.[310]

Furthermore, the dynamics and dependencies of this environment are constantly churned by the current political climate, changing social context, and even operational outcomes. Not only that, but executive interpretation of legislation is subject to change and greatly affects when and how government departments and agencies leverage authorities to accomplish the goals of the executive administration. There is often a complex relationship between policy and legislation that is supplemented by innumerable amendments and repeals.[311] Incomprehensive as it may be for present discussions, it shows the volatility with which policy, strategy, and even organizational identity change

---

[309] *See* WHY OVERCLASSIFICATION OCCURS. Elizabeth Goitein and David M. Shapiro, "Reducing Overclassification Through Accountability," paper from the Brennan Center for Justice, New York University School of Law (New York: New York University, 2011), 21–32, http://www.brennancenter.org/sites/default/files/legacy/Justice/LNS/Brennan_Overclassification_Final.pdf. *See* also *supra* note 85.

[310] *See* 13.3 UNITY OF EFFORT IN SHARING INFORMATION. Thomas H. Kean and Lee Hamilton, *et al.*, *The 9/11 Commission Report*, report submitted by the National Commission on Terrorist Attacks Upon the United States (Washington DC: GPO, 2004), 1416–19. "Security concerns need to be weighed against the costs. Current security requirements nurture overclassification and excessive compartmentalization of information among agencies. Each agency's incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information. No one has to pay the long-term costs of overclassifying information, though these costs—even in literal financial terms—are substantial. There are no punishments for *not* sharing information. Agencies uphold a "need-to-know" culture of information protection rather than promoting a "need-to-share" culture of integration" (author's emphasis).

[311] *See* FIGURE 3.1: EVOLUTION OF POLICY. La Bash and Landis, 14.

when compared with the significantly more stable course of legislation. Thus, the role of policy is necessary, but it does not factor in to current discussions with the same force of permanence that characterize examinations of legislation.

Another consideration that frustrates inter-title cooperation is that as policy is created, it often seeks to avoid the precarious overlap between operations conducted on foreign soil and those conducted in defense of the homeland. These are especially pronounced in the areas of Homeland Security and counterterrorism. Even when developing policy for foreign intelligence operations in isolation from all else, however, there are concerns that must distinguish between traditional military operations and foreign intelligence gathering—the latter of which occurs under significantly more stringent requirements.[312] The difficulties associated with forming and reforming these policies to address evolving threats are numerous, but recent policy interpretations of cyberspace-relevant legislation has arguably favored inter-title cooperation more often than not.[313]

Policies, therefore, provide an indication of the current course and direction that current executive administrations are taking and represent the potential for future administrations. Guantanamo is an excellent example of the potential of policy across administrations. On November 13, 2001, President George W. Bush signed a military order to convene a military tribunal that effectively turned the military base at Guantanamo Bay into a detention facility for alleged terrorists.[314] Over eight years later, in response to this, President Barak Obama issued EO 13492[315] calling for the prompt closure of the detention facility

---

[312] *See* OVERSIGHT & COMPLIANCE. *Infra* at Ch. 4 s. (A).

[313] EO 12127, EO 12333, EO 13493, EO 13519, EO 13584, EO 13603, EO 13629, EO 13636, EO 13688, EO 13691, PPD-1, PPD-2, PPD-8, PPD-14, PPD-18, PPD-20, PPD-21, PPD-23, etc. Notably, PPD-28 likely deconstructs some interagency cooperation as it relates to Signals Intelligence collection conducted under the purview of the NSA pursuant to 50 USC §§ 3038(b)(1) as specified in EO 12333 s. 1.7(c).

[314] F.R. vol. 66, no. 222, pt. IV, "Military Order of November 13, 2001—Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism" (November 16, 2001): 57831–57836.

[315] F.R. vol. 74, no. 16 (January 27, 2009).

after assigning an official disposition to those who were being detained. Just over two years after that order was issued, President Barak Obama followed it up with EO 13277,[316] which allowed for continued detention of prisoners under similar justifications as President George W. Bush nearly a decade earlier. No significant legislative changes demanded these policy issuances, but the presidential policy, in each case, gave a definitive—albeit sometimes short-lived—direction to executive agencies based upon current circumstances and future goals.

Additionally, policy provides benchmarks, which provide active feedback for legislators. If policy goes too far, the judiciary should step in and put a halt to it. If it goes in an undesirable direction, then legislators serve to provide course corrections. In either case, the law remains the foundational principle and policy can often be more quickly adjusted to more effectively pursue national interests and provide national security.

2. Examples of Inter-Title Cooperation

The following discussions will address some notable inter-title events, lessons from which will be applied to inter-title cooperation as it relates to cyberspace operations. These operations are not exhaustive nor do they contain the enumerable inter-title operations that preclude an examination due to classification requirements.

The Los Angeles Riots of 1992 saw support from State and Local Law Enforcement (SLLE), The National Guard, U.S. armed forces, the U.S. marshals, and the FBI. These consolidated forces are one of the largest inter-title operations to be enforced under a federalized state of emergency. The challenges posed to this short-fused operation provide insight into force organization and communications during inter-title operations.

Federal emergency response efforts addressing the devastation left by Hurricane Katrina in 2005, which was responsible for nearly 2,000 U.S. deaths

[316] F.R. vol. 76, no. 47 (March 10, 2011).

and over $150 billion in damages.[317] The highly criticized response saw support from numerous agencies operating under at least five title authorities to provide responses to displaced populations originating throughout "all of the coastal counties of Louisiana, Mississippi and Alabama" and extending "well inland" throughout area of Louisiana, Mississippi, and Alabama.[318]

While not linked to any specific event, select activities in the War on Terrorism will be examined since most of them include Title 50 authorities both domestically and abroad. The NSA, CIA, FBI, U.S. armed forces, National Guard, Coast Guard, and DHS all proudly broadcast the pooling of their combined expertise, equipment, and efforts that have reduced the threat of terrorism to the United States and her allies. This examination will be complemented by a brief overview of some *Homeland Security* efforts in terms of exercises and events that show the extent to which DHS intends to leverage interagency cooperation to ensure the adequacy of various homeland defense measures.

a. L.A. Riots

On April 29, 1992, following the controversial acquittal of four Police Officers accused of unlawful conduct against the now-prominent Rodney King, riots broke out across large portions of Los Angeles, California. For the purposes of this examination, the causes of the riots are less significant than the government responses—specifically those that involved multiple title authorities supporting the same operation. The initial hours of rioting began around 1630 and were addressed by mostly SLLE. A little over four hours later, however, California governor, Pete Wilson, formally requested the mobilization of 2,000 National Guard troops from the Adjutant General. Complete mobilization took another 18 hours, but by 1500 the following day, National Guard troops operating under SAD authorities were supporting law enforcement efforts across the city of

---

[317] *See* generally United States Census Bureau, "Profile America Facts for Features: Hurricane Katrina 10th Anniversary," No. CB15-FF.16 (Washington DC: DOC, 2015), https://www.census.gov/newsroom/facts-for-features/2015/cb15-ff16.html.

[318] Ibid.

Los Angeles. There were ongoing and lingering debate about whether the National Guard was needed to supplement the resource shortage or to remedy the city's resource mismanagement.[319] Regardless, the SAD had been authorized and the governor was funding the deployment of the state's militia to quell city-wide rioting. Escalating violence over the next eight hours led to an official governor's request for federal troops at just after midnight on the first of May.[320]

When the request had reached the White House, President George H.W. Bush authorized the deployment of 4,000 armed forces personnel by Executive Order[321] pursuant to provisions in the Insurrection Act.[322] In addition, the president ordered DOJ to make 2,000 special riot-control units available to the ongoing operation from the FBI and the U.S. Marshals. Nearly 24 hours after the initial mobilization of troops under the authorities of California State Active Duty, Joint Task Force Los Angeles (JTF-LA) was formed with SLLE, National Guard (32 USC),[323] and U.S. armed forces (10 USC), and members of the FBI and U.S. Marshals (18 USC).[324]

Despite the successes in deploying the vast forces of diverse personnel, the operation struggled from disunity in effort and a lack of clear command and control. Since the president had leveraged authorities under the Insurrection Act,

---

[319] *See* generally Susan Rosegrant,"The Flawed Emergency Response to the 1992 Los Angeles Riots," case study in *Executive Session on Domestic Preparedness, John F. Kennedy School of Government*, no. C16-00-1586.0 (Cambridge, MA: Harvard University, 2000), 3–6, http://www.ksg.harvard.edu/research/publications/cases/1586_0.pdf.

[320] *See* generally James Delk, *Fires & Furies: The L.A. Riots, What Really Happened* (Palm Springs, CA: ETC, 1995), 55–60.

[321] EO 12804

[322] 10 USC §§ 331, *et seq.*

[323] Ibid. In the case of the L.A. Riots, National Guard personnel were "federalized' and transitioned into a Title 10 authority with statutory exception to the PCA. Depending on their employ, however, they could have easily remained under 32 USC authorities and coordinated or supported 10 USC activities. For further discussion, *see* HURRICANE KATRINA. *Infra* at Ch. 3 s. (A)(2)(b).

[324] George H.W. Bush, "Address to the Nation on the Civil Disturbances in Los Angeles, California," May 1, 1992, online by Gerhard Peters and John T. Woolley, *The American Presidency Project*, http://www.presidency.ucsb.edu/ws/?pid=20910.

the operation became federalized and eventually was placed under the command of Army General Marvin Covault.[325] The implications of this were relatively clear between the armed forces and the National Guard, but there appeared to be little understanding of how to integrate federal efforts with the SLLE.[326] Many of the reports that were consolidated in the aftermath of the L.A. Riots suggested that there were major deficiencies in training that caused federal troops—especially in the armed forces—to be unsure of how to properly assist or conduct law enforcement activities.[327] All parties appeared to clearly understand the need for unity of effort and a clear chain of command. Within the federal ranks, however, only the National Guard appeared to understand the "mission requirements, constraints, and interagency operations better than the active duty commanders."

Misunderstandings were a significant hurdle that impaired the overall effectiveness of the operation and led to disjointed efforts throughout the operation. This theme of clear lines for responsibility and authority are not only important to operational efficiency, but they are, in most cases, a requirement of the law. In every case, the spectrum of responsibility and extent of authorities demands that operators be trained to clearly understand the expectations and limitations of their involvement based on the spectrum of authorities involved in the operation.

---

[325] *See* OPERATIONAL CONSTRAINTS. William W. Mendel, "Combat in Cities: The LA Riots and Operation Rio," (Fort Leavenworth, KS: Foreign Military Studies Office, 1996) http://fmso.leavenworth.army.mil/documents/ rio.htm. "Ultimately, the Guard deployed 10,465 troops that were subsumed by Joint Task Force-Los Angeles Headquarters. JTF-LA was put together by the Regular Army's U.S. Forces Command in Atlanta which assigned 2,023 troops from the 7th Infantry Division and 1,508 Marines from Camp Pendleton. This was not much of an increase, but it was enough to put a federal officer in charge."

[326] *See* OPERATIONAL CONCEPT AND TACTICS. Ibid.

[327] *See* CONCLUSIONS. Ibid. *See* also Rosegrant, 4–15. *See* also John H. Ebbighausen, "Unity of Command for Homeland Security: Title 32, Title 10, Or A Combination," (master's thesis, U.S. Army Command and General Staff College, 2006), 49–59, http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA451789.

b. Hurricane Katrina

On August 29, 2005, Hurricane Katrina made landfall as a Category 3 hurricane near the Louisiana-Mississippi border. This was its third landfall, but the storm had still not substantially diminished in strength. The ensuing devastation would accrue over $100 billion in damages and claim the lives of over 1,200 people. It was not only one of the worst natural disasters in recent memory, but in the history of the United States.[328] The event timeline preceded Katrina's landfall by three days when, in anticipation of the impending storm, the Louisiana governor's office declared a state of emergency and subsequently activated 4,000 National Guard personnel under SAD authorities. Mississippi soon followed suit and activated near as many with 2,500 from their National Guard.[329] On August 27, 2005, President George W. Bush responded to the two governor's federal-aid requests by declaring Louisiana a federal disaster area and invoking authorities available pursuant to the Stafford Act.[330]

In response to this, United States Northern Command (USNORTHCOM) began forming pieces of what would later officially constitute Joint Task Force Katrina (JTF-Katrina).[331] In contrast to the Los Angeles Riots, there was a significantly greater lead time for planning and coordination; however, the sheer geographic extent and unforeseen complexity of factors that characterized this disaster led to widespread criticism of what amounted to mostly reactionary

---

[328] *See* generally Christine Gibson, "Our 10 Greatest Natural Disasters," *American Heritage* 57, no. 4 (August/September 2006), http://www.americanheritage.com/content/our-10-greatest-natural-disasters.

[329] U.S. Library of Congress, Congressional Research Service, *Hurricane Katrina: DOD Disaster Response*, by Steve Bowman, Lawrence Kapp and Amy Belasco, RL33095 (2005), https://www.fas.org/sgp/crs/natsec/RL33095.pdf.

[330] Stafford Act (42 USC §§ 5121, *et seq.*)

[331] *See* USNORTHCOM'S SPECIFIC MISSION. "About USNORTHCOM," United States Northern Command, accessed March 11, 2016, http://www.northcom.mil/AboutUSNORTHCOM.aspx. "USNORTHCOM's civil support mission includes domestic disaster relief operations that occur during fires, hurricanes, floods and earthquakes. Support also includes counter-drug operations and managing the consequences of a terrorist event employing a weapon of mass destruction. The command provides assistance to a Primary Agency when tasked by DOD. Per the Posse Comitatus Act, military forces can provide civil support, but cannot become directly involved in law enforcement."

responses. When Katrina made landfall on August 29, then President George W. Bush issued an emergency declaration and the Secretary of DHS, Michael Chertoff, in turn declared Hurricane Katrina to be an "Incident of National Significance."[332] These and other developments led to the National Guard being transitioned from a state-funded status (under SAD) to a federally funded National Guard status (32 USC), which allowed them to remain operational and under the control of the state governor. One legislative development that allowed for the states to surge their response capability came in 1996 when Congress passed consent to the Emergency Management Assistance Compact (EMAC).[333] This law effectively allowed states to pool resources, including police, fire, medical services,[334] and state militia[335] to improve responses to exceptionally challenging emergency disasters.[336]

From a federal perspective, the EMAC appears to limit the number of federal options in responding to events where EMAC has been activated. These complications derive from the legislation's specific prohibition against the use of the National Guard for Title 32 operations outside their home state. Due to the wording of the EMAC legislation, which reads, "nothing in this compact shall authorize or permit the use of military force by the National Guard of a State at any place outside that State in any emergency for which the president is authorized by law to call into federal service the militia," it may appear that once the National Guard are transitioned to Title 32 authorities, they are unable to perform duties on behalf of any state except their own. A more careful reading suggests, however, that so long as the militia remains under the authority of the governor, they appear to avoid the "military force" prohibition and are authorized

[332] Pursuant to 42 USC § 5184.

[333] Pub. L. 104–321

[334] *Id.* at Art. VII

[335] *Id.* at Art. I, s. 1

[336] Ibid.

to perform “other duties” as stipulated in 32 USC.[337] This interpretation appears consistent with the Hurricane Katrina report for Congress.[338]

For cyberspace operations, this becomes of critical importance. If USCYBERCOM is able to establish a National Guard capability under the Cyber Protection Forces, then any mission-capable teams will likely have statutory authorization under EMAC to perform “other duties” in a federally funded role (32 USC) to respond to state requirements for cyber emergency disasters. Additionally, under provisions in 10 USC, these National Guard teams would likely be able to utilize DOD facilities in order to deliver these requirements.[339]

In the case of Katrina, however, the EMAC provisions that enabled the deployment of nearly 46,000 National Guard personnel to provide emergency relief to Mississippi and Louisiana,[340] were deemed by most critical examinations to have fallen short of success. In keeping with the National Response Plan,[341] the DOD prevented itself from adequately counteracting the state governors’ severe miscalculations in response requirements. Furthermore, when a DOD response was initiated, it was apparently done without coordinating with FEMA.[342] In addition to the irregular aspects of some DOD response efforts, the Louisiana governor, Kathleen Blanco, refused to allow the commander of JTF-Katrina (10 USC) to take control of evacuation efforts or unify command of the National Guard under his authority.

---

337 Pursuant to 32 USC § 502(f).

338 *See* ROLE OF THE NATIONAL GUARD. CRS, *Hurricane Katrina: DOD Disaster Response*, 6–11.

339 Pursuant to 10 USC § 372(a).

340 *See* TABLE 1. CRS, *Hurricane Katrina: DOD Disaster Response*, 11.

341 Secretary of Homeland Security, *National Response Plan, 2004* (Washington DC: DHS, 2004), https://it.ojp.gov/fusioncenterguidelines/NRPbaseplan.pdf.

342 *See* ISSUES FOR CONGRESS. CRS, *Hurricane Katrina: DOD Disaster Response*, 13.

There are a great number of examinations as to why Hurricane Katrina relief efforts failed to achieve a successful response threshold.[343] Many of the complexities that derailed Hurricane Katrina relief efforts were founded in ambiguous or ill-suited legislation. Since USNORTHCOM (10 USC) was commanding JTF-Katrina, many saw it as being precluded by the Posse Comitatus Act from directing Title 32 in law enforcement efforts.[344] More than that, there was no clear precedence for USNORTHCOM to unify command and control over the United States Coast Guard (14 USC) assets or any of the FEMA (6 USC) efforts. In retrospect, given the severe impotence of Louisiana SLLE, the president arguably had statutory authority under the Insurrection Act[345] to federalize forces where he could reasonably establish an absence of the rule of law—the Louisiana Superdome being a prime example.[346] This arguably would have allowed USNORTHCOM to direct all efforts in defense of the state and to more closely support the U.S. Coast Guard and FEMA relief efforts. This observation may appear inappropriate given that Hurricane Katrina responses were primarily focused on relief efforts, with restoral of order being a secondary concern. This decision to place USNORTHCOM over all federal operations, however, is more closely linked to their surge capacity in terms of mobility, staffing, and coordination than any other factor. If DHS had the staffing and surge capacity, JTF-Katrina could arguably be more directly employed by the Secretary

---

343 *See* generally Christopher Cooper and Robert Block, *Hurricane Katrina and the Failure of Homeland Security* (New York: Henry Holt, 2006). *See* also HURRICANE KATRINA AND THE UNLEARNING OF LESSONS. Thomas Birkland, *Lessons of Disaster: Policy Change after Catastrophic Events* (Washington DC: Georgetown University Press, 2006), 182–90.

344 *See* Ebbighausen, 60–61.

345 10 USC § 331, et seq.

346 *See* generally Mark Egan, "Rapes, Killings Hit Katrina Refugees In New Orleans," *Reuters*, September 4, 2005, archived at http://www.redorbit.com/news/general/229546/rapes_killings_hit_katrina_refugees_in_new_orleans. *See* also John Burnett, "More Stories Emerge of Rapes in Post-Katrina Chaos," *National Public Radio*, December 21, 2005, http://www.npr.org/templates/story/story.php?storyId=5063796.

of Homeland Security, though likely still under the operational control of USNORTHCOM.[347]

Though his choice of wording is regrettable, Assistant Secretary of Defense for Homeland Defense, Paul McHale pointed out that the National Defense Authorization Act of 2004[348] enabled,

> a single National Guard officer [to be] given […] dual-hatted command. He was placed in Title 32 status to command the Title 32 forces [and] was placed simultaneously in Title 10 status under the command and control of the combatant commander so that unity of effort could be achieved, even though we maintained the distinction in terms of unity of command.[349]

Significantly less is known about the FBI's involvement in Hurricane Katrina relief efforts despite their claim that over 500 of their agents were consolidated from around the country to, "secure the city, answer emergency calls, patrol the streets, conduct search and rescue operations, and identify victims."[350] As such, it is difficult to fold their operations into and understand them under the overall scrutiny of inter-title operations that characterized the experiences of DHS, DOD, and SLLE.

Subsequent legislation—most notably, the National Defense Authorization Act of 2010[351]—would eliminate many of the remaining statutes that were seen as mutually excluding unity of command during inter-title operations. In addition

---

[347] *See* PRINCIPAL FEDERAL OFFICIAL. Secretary of Homeland Security, "National Response Plan," 33–34. This is consistent with the NRP that was developed and released eight months prior to the Hurricane Katrina disaster.

[348] Pub. L. 108-136

[349] Paul McHale, "Hearing on Department of Defense Homeland Security Responsibilities," before the *House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities*, March 15, 2005, in Congressional Research Service, *Hurricane Katrina: DOD Disaster Response*, 10–11.

[350] *See* A NEW ERA OF NATIONAL SECURITY, 2001–2008. Federal Bureau of Investigation "The FBI: A Centennial History, 1908–2008," (Washington DC: GPO, 2008), 98–115, https://www.fbi.gov/about-us/history/a-centennial-history/the-fbi-a-centennial-history-1908-2008. "In the months that followed, the Bureau led a series of public safety initiatives to support area law enforcement and teamed up with local and federal authorities in the region and around the nation to stem the flood of scams preying on hurricane victims."

[351] Pub. L. 111-84

to poor cooperation between personnel operating under Title 10 and Title 32 authorities, FEMA was harshly criticized in the aftermath of Katrina for their anemic natural disaster response and coordination capability, which was neglected as a result of the heavy emphasis being placed on terrorism prevention and preparedness since the 9/11 attacks.[352]

c. Homeland Security: Counterterrorism

One of the difficulties in addressing terrorism is that it possesses no universally accepted definition.[353] To pair it with the nebulous descriptions often associated with cyberspace make the task of applying legal frameworks to cyberterrorism a nearly insurmountable task. For one, domestic and international interpretations of terrorism are still steeped in the national liberation movements that characterized the 20th century and no clear consensus has adequately surmised the nature of the current terrorist threat.[354] Additionally, there is still great diversity in how terrorism is legally approached. In some cases of federal law, terrorism and its various aspects are seen as an act of war[355] while other instances of terrorism are considered to be criminal in nature.[356] With its broad punitive authorities and ambiguous definitions, federal counterterrorism efforts generate an endless supply of legal analyses.

Armed Forces Counterterrorism: Given the declaration of a "War on Terror," by President George W. Bush in 2001, the armed forces seemingly need

---

[352] *See* EXECUTIVE SUMMARY. Office of Inspections and Special Reviews, *A Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina* (Washington DC: DHS, 2006), 1–3, https://www.oig.dhs.gov/ assets/Mgmt/OIG_06-32_Mar06.pdf.

[353] Even domestic and international terrorism as defined by the United States Code have nuanced differences between the various title authorities (c.f., 6 USC § 101(16), 18 USC §§ 2331,2332b, 22 USC § 2656f(d), 50 USC § 1801(c), *et al.*)

[354] *See* TERRORISM AND THE UN: AN AMBIVALENT RELATIONSHIP. Jackson Nyamuya Moagoto, *Battling Terrorism: Legal Perspectives on the Use of Force and the War on Terror*, (New York: Routledge, 2005), 54–55.

[355] Pursuant to 10 USC §§ 821,836,950t and 50 USC § 1541.

[356] *See* generally 18 USC §§ 2339,2339A,2339B,2339C governing material support to terrorism. *See* also *id.* at §§ 844,922,924 governing explosives offenses. *See* also *id.* at § 956 governing conspiracy to murder, kidnap, or maim persons or to damage property overseas.

no additional authorities to conduct counterterrorism operations. However, ambiguity under Geneva conventions[357] and the primary employment of the armed forces as the standing military have led to significant changes in legal interpretation. As alluded to earlier, Title 10 takes advantage of an interpretation of terrorism that sees some individual acts of terrorism as part of a "broader campaign of violence directed against the state."[358] Current interpretations still lack support for using traditional Geneva Conventions' definitions to justify counterterrorism as a response to an international armed conflict. This, however, has not dissuaded efforts that find significantly more traction under resolutions establishing a nation's inherent right to self-defense.[359] With a significantly greater capacity for effectiveness there is justification for understanding terrorist acts as threatening "territorial integrity or political independence."[360]

Along these lines, Operation Neptune Spear,[361] taking place on May 2, 2011, and leading to the death of Osama Bin Laden, presents an interesting case study for the justifiability of inter-title operations in support of counterterrorism. At the time, Leon Panetta was the Director of the CIA—soon to be named Secretary of Defense—and was quick to clarify that the raid had been conducted under Title 50 authorities.[362] This oft-cited distinction epitomizes proponents and detractors alike in assessing the appropriateness of inter-title operations. This

---

[357] *See* generally, Joan Fitzpatrick, "Jurisdiction of Military Commissions and the Ambiguous War on Terrorism," *The American Journal of International Law* 96, no. 2 (April 2002), pp. 345–354.

[358] *See* LAW OF WAR APPLIED. U.S. Library of Congress, Congressional Research Service, *Terrorism and the Law of War: Trying Terrorists as War Criminals before Military Commissions*, by Jennifer Elsea, RL31191 (2001), 10–11, http://fpc.state.gov/documents/organization/7951.pdf.

[359] 1945 U.N. Charter, Article 51.

[360] *Id.* at Article 2(4). *See* also THE CONFLICT MANAGEMENT PARADIGM: TERRORISTS AS WARRIORS. Moagoto, 66–75.

[361] *See* generally "Operation Neptune Spear (2011)," *Shadowspear: Special Operations,* accessed March 11, 2016, http://www.shadowspear.com/2011/05/operation-neptune-spear-bin-laden. Neptune Spear was the code name for the Abbottabad operation in which CIA and U.S. Special Forces raided a compound housing Osama Bin Laden, which resulted in his death.

[362] *See* generally Leon Panetta, interview by Jim Lehrer, *PBS New Hour*, May 3, 2011, http://www.pbs.org/newshour/bb/terrorism-jan-june11-panetta_05-03.

"either-or" concept—i.e., either "Title 50" or "Title 10"—is the product of an imprecise policy and is not a necessary distinction precipitated by the law. In the case of the Bin Laden raid, so long as Title 50 and Title 10 oversight requirements are met and the authorities authorize the actions, there are no glaring issues that would prevent the integration of inter-title forces for an operation that provides a mutual advantage to both forces.[363]

CIA Counterterrorism: One of the more controversial programs executed under the federal counterterrorism mission is the CIA's use of drones under the presidential direction. After more than a decade of operational successes, this mission set—often referred to as the "CIA Drone Program"—remains the subject of numerous editorials and a host of legal scrutiny. This "new age" of counterterrorism has seen a resurgence in CIA activity, which uses covert action to achieve foreign policy objectives and support national security objectives under Title 50 provisions.[364] Far from the world of traditional espionage, however, the CIA has projected a more military-like persona as they have made use of drones that were originally developed for employment by the armed forces. These operations are undergirded by precarious legal interpretations that do not appear to be able to be applied consistently. In the first place, the justification derives from the president's authority to conduct covert action so long as it is delivered through approved federal appropriations and congressional reporting requirements are met.

While seemingly simple, the definition of "covert action" presents a nagging contradiction to the counterterrorism discourse since its stipulation that "the role of the United States Government will not be apparent or acknowledged

[363] This conclusion is purposefully overstated. There are fiscal concerns, and *de jure* prohibitions that are unique to many instances of inter-title cooperation. In the case of Operation Neptune Spear, however, most of these concerns were not present in applicable law. *See* INTRODUCTION. Wall, 85–87. *See* also Robert M. Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of National Security Law & Policy* 5 (2012): 539–44.

[364] Pursuant to 50 USC § 3093.

publicly"[365] is all too often disregarded. Some more notable examples of this include the publicly issued authorizations for the CIA to conduct drone strikes that killed Anwar al-Awlaki and his 16-year-old son, Abdulrahman al-Awlaki in 2011.[366] To complicate matters further, there is an additional prohibition against conducting covert actions that are considered traditional military activity.[367] Even still, executive authorities are likely to provide themselves with a certain amount of leeway in affirming adherence to these legal distinctions, even when the operational means and methods used by each title authority may be the same.[368]

Previous examples have illuminated close inter-title cooperation between the armed forces and the CIA, with the presumed support of the NSA as a co-Title 50 authority. By contrast, the CIA and FBI share a much more checkered past. Their oft-defunct relationship was a recurring theme in final report from the 9/11 Commission,[369] though current reports seem to indicate a positive trend between the two historically discordant agencies.[370]

FBI Counterterrorism: The primary goal of the FBI is to use federal avenues for legal prosecution to disrupt support for terrorism and terrorist activities. Since every major terrorist organization is reliant on the same global

---

[365] *Id.* at § 3093(e).

[366] *See* generally Greg Miller, "Muslim Cleric Aulaqi Is 1st U.S. Citizen On List of Those CIA Is Allowed To Kill," *Washington Post*, April 7, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/04/06/AR2010040604121.html. The kill order for the two al-Awlakis was more controversial because it raised questions about the legality of authorizing the killing of U.S. citizens abroad.

[367] 50 USC § 3093(e)(2).

[368] This is not an entirely unreasonable prospect. The CIA, NSA, Armed Forces, and FBI have significant similarity in the ways and means of executing their respective title authorities. Weapons, surveillance, security, tactics, and policy can be very similar even if the underlying authorities are different.

[369] *See* ADAPTATION—AND NONADAPTATION—IN THE LAW ENFORCEMENT COMMUNITY. Kean and Hamilton, *et al.*, "The 9/11 Commission Report," 73–82. *See* also *id.* at 423–28.

[370] *See* generally Bruce Hoffman, Edwin Meese III and Timothy J. Roemer, "The FBI: Protecting the Homeland in the 21st Century," report of the congressionally-directed *9/11 Review Commission* to the Director of the Federal Bureau of Investigation (Washington DC: GPO, 2015), 15–37, https://www.fbi.gov/stats-services/publications/protecting-the-homeland-in-the-21st-century.

support networks as the United States, the FBI is able to employ a wide variety of statutory authorities. Many of these authorities came as a direct result of amendments contained in the USA PATRIOT Act of 2001. These expanded authorities have allowed the FBI to increase counterterrorism efforts pursuant to previously discussed statutory amendments to FISA and the ECPA. In addition to these, amendments to laws authorizing the issuance of National Security Letters (NSL)[371] have enabled the FBI to advance investigations through increased collection against domestic and international terrorists.[372] Above all else, the increased provisions of the USA PATRIOT Act have served to break down the "perceived barrier wall that had impeded the sharing of information between intelligence and criminal investigators."[373]

These new authorities and expanded definitions for terrorism[374] have authorized investigators to compliment counterterrorism efforts primarily by prosecuting acts that target individual citizens or groups as well as disrupting material support and the delivery of weapons and ordinance.[375] Relevant statutory authority preemptively compliments counterterrorism efforts by allowing the FBI to target illicit supply chains and intervene during the critical stages of recruitment and planning. Efforts against these supply networks add value to other organizations—the armed forces, U.S. Coast Guard, DHS, intelligence agencies, etc.—in that they are often responsible for identifying persons of

---

[371] 12 USC § 3414(a)(5)(A), 15 USC §§ 1681u,1681v, 18 USC § 2709, and 50 USC § 436.

[372] *See* generally Gabriel Malor, "Cut the Crap, Apple, and Open Syed Farook's iPhone," *The Federalist*, February 19, 2016, http://thefederalist.com/2016/02/19/cut-the-crap-apple-and-open-syed-farooks-iphone. Statutes pertaining to NSL were one of the primary authorities behind the FBI's court order demanding Apple, Inc. to assist the federal government in accessing the phone of deceased domestic terrorist, Syed Farook. *See* also *United States of America v. Apple, Inc.*, in Hearing On Government's Motion to Compel Apple Inc. To Comply With This Court's February 16, 2016 Order Compelling Assistance In Search in U.S.D.C. C.D.C., CM 16-10 (2016), https://www.justice.gov/usao-cdca/file/826836/download. The FBI used additional provisions pursuant to the All Writs Act (28 USC § 1651) to compel Apple, Inc. to provide technical assistance as a third party in obtaining the evidence of Farook's iPhone.

[373] Hoffman, *et al.*, 25.

[374] Definitions for domestic and international terrorism are contained in 18 USC § 2331. The federal crime of terrorism is further defined in 18 USC § 2332b.

[375] *See supra* note 355. *See* also 18 USC §§ 1203,2332 which concern hostage taking and terrorist acts abroad against U.S. citizens—including murder.

interests that compliment ongoing operations being conducted by other title authorities. There are also additional statutory authorities that are designed to be directly complimentary to inter-title operations in the areas of international terrorism[376] and weapons of mass destruction.[377]

Overall, the broad authorities of the FBI allow them to gather relevant information through a variety of criminal investigations[378] and to compliment counterterrorism operations by disseminating relevant information to other agencies and organizations.[379] The FBI also has the added benefit that their threshold for initiating investigations and gathering evidence tends to be one of the strictest amongst their inter-title counterparts. This suggests that any information they contribute is unlikely to disrupt or derail operations based on the myriad of rules of evidence or investigative procedure that their partners are operating under.

DHS Counterterrorism: Counterterrorism is the cornerstone of the DHS homeland security mission[380] and was the primary reason for their creation under the Homeland Security Act of 2002[381] following the September 11 attacks in 2001. Under Title 6 authorities, DHS pursues both global and domestic terrorism that threaten national security. Though DHS is charged with preventing and assisting in recovery from terrorist attacks, "primary responsibility for investigating and prosecuting acts of terrorism" are vested in "federal, State, and local law enforcement agencies with jurisdiction over the acts in question."[382]

---

[376] Pursuant to 18 USC § 2332b. Statues apply to terrorism that transcends national boundaries.

[377] *Id.* at § 2332a.

[378] For instance, cybercrime, identity theft, immigration violations, and even perjury.

[379] *See* TESTIMONY OF THE HONORABLE ROBERT S. MUELLER, III. U.S. Congress, Senate, Committee On The Judiciary, *The War Against Terrorism: Working Together to Protect America*, 108th Cong., 1st sess., 2013, https://www.judiciary.senate.gov/imo/media/doc/mueller_testimony_03_04_03.pdf.

[380] 6 USC § 111(b)(1)

[381] Pub. L. 107-296.

[382] 6 USC § 111(b)(2)

This can pose a number of challenges for DHS, which relies heavily upon a robust network of coordination centers to fulfill their statutory requirements. The cyber-coordination capability that exists under the NCCIC, however, has overlap and compatibility with similar watch floors at the National Counterterrorism Center (NCTC), the National Counter Proliferation Center (NCPC), and the National Intelligence Centers (NIC), all of which operate under the Office of the Director of National Intelligence (ODNI).[383]

DHS operates under authorities derived from a vast collection of laws and regulations. Within the bounds of terrorism prevention, they are authorized to make relevant databases available to businesses in order to alleviate work status concerns for current or new employees.[384] Under the Homeland Security Appropriations Act of 2007,[385] they can establish "risk-based performance standards" to improve security at high-risk chemical facilities and propose legislation for improved chemical distribution regulations.[386] Under Critical Infrastructure Information authorities[387] and CISA, DHS can more easily facilitate the sharing of information between the owners and operators of the critical infrastructures and relevant government agencies that are involved in infrastructure protection and counterterrorism. There are additional, though limited provisions for DHS to affect travel procedures as well as authorities that relate to prevention and response measures for bioterrorism.

---

[383] Pursuant to 50 USC § 3056, *et seq.*, the following centers have information sharing partnerships with Central Intelligence Agency: Defense Intelligence Agency, Department of Agriculture, Department of Defense, Department of Energy, Department of Health & Human Services, Department of Homeland Security, Department of Justice, Department of State, Department of the Treasury, Drug Enforcement Administration, Federal Bureau of Investigation, National Geospatial Intelligence Agency, Nuclear Regulatory Commission, National Security Agency, Transportation Security Administration, and the U.S. Capitol Police among others.

[384] Pursuant to 8 USC § 1324a

[385] Pub. L. 109-295

[386] *See* AMMONIUM NITRATE SECURITY PROGRAM; PROPOSED RULE. F.R. vol. 76, no. 149 (August 3, 2011).

[387] 6 USC §§ 131, *et seq.*

Conclusions on Counterterrorism: Some of the preceding observations may convey a critical view of ongoing operations for certain organizations—most notably the CIA. These observations, however, are not intended to argue for the negation of inter-title cooperation, but rather, they demonstrate that, in the case of counterterrorism, there are ongoing legal concerns that apply uniquely to each title authority. Whether by injudicious application or legislative ambiguity, these unique legal concerns may lead to inappropriately enabling or constraining inter-title operations. As it is increasingly unlikely that terrorist organizations will cooperate with federal attempts to resolve hostilities by means of peaceful discourse, there is an increasing necessity for the United States to comprehend the nature of its victimization and to defend itself appropriately without resorting to blatant and unlawful acts. As legislation and the context for these legal interpretations change, the framework for inter-title cooperation is likely to be affected as it pertains to counterterrorism.

d. Homeland Security: Critical Infrastructure Protection (CIP)

The importance of CIP is obvious from the central role that it plays in policy and legislation. When Leon Panetta used the term, "cyber Pearl Harbor," he was not imagining a decisive assault against the U.S. military complex as the genuine event of 1941 proposed to be. Instead, speaking with business executives in New York City, he forecasted a future where cyberspace will be used to derail passenger trains and chemical shipments. Additional foreboding descriptions saw the poisoning of metropolitan water supplies and "several attacks on our critical infrastructure at one time, in combination with a physical attack on our country."[388] Panetta's ominous vision embodies much of the underlying emotion that underpins CIP efforts—not least of these efforts are the policy and legislation themselves. The "lack of imagination" that contributed to the sheer shock and surprise shared by federal employees and civilians is

[388] *See* generally Leon E. Panetta, "Remarks on Cybersecurity" (speech, Business Executives for National Security, New York, October 11, 2012) published in *Council on Foreign Relations*, October 12, 2012, http://www.cfr.org/cybersecurity/secretary-panettas-speech-cybersecurity/p29262.

something that the United States appears keen to prevent from happening again.[389]

It is not just terrorism, however, that informs measures in CIP and the broader framework for national security. The surprise of terrorist attacks may have provided the level of motivation needed to institute broad and necessary changes, but serious approaches to domestic homeland security existed long before the fateful events of September 11, 2001.[390] The U.S. Commission on National Security/21st Century—known as the Hart-Rudman Commission—was started in 1998 by then Secretary of Defense William Cohen. Their final report, which was a culmination of more than three years' worth of work, was published in February of 2001—nearly a full seven months before 9/11. The report, *Road Map for National Security: Imperative for Change*, called for numerous improvements including the development of a strategic framework for homeland security,[391] an organizational realignment that supported homeland security efforts,[392] and the need for executive-legislative cooperation[393] to ensure its effectiveness. All of these themes have been hallmarks of extensive efforts that have led to an expansion of inter-title cooperation in the area of 21st-century homeland security and specifically, Critical Infrastructure Protection.

CIP is primarily a function of Title 6 authorities,[394] but it involves large portions of the civilian sector and almost every major executive department and subordinate agency in the federal government. USNORTHCOM and United States Southern Command (USSOUTHCOM) are some of the more notable title-

---

389 *See* FORESIGHT—AND HINDSIGHT. Kean and Hamilton, *et al.*, "The 9/11 Commission Report," 339. The Commission reported that "the 9/11 attacks revealed four kinds of failures: in imagination, policy, capabilities, and management."

390 Gary Hart and Warren B. Rudman, *Road Map for National Security: Imperative for Change*, report submitted by the U.S. Commission on National Security/21st Century (Washington DC: GPO, 2001). http://govinfo.library.unt.edu/nssg/PhaseIIIFR.pdf.

391 *Id.* at 11.

392 *Id.* at 14.

393 *Id.* at 26.

394 *See supra* note 386.

10 organizations that make up the federal consortium, though every COCOM arguably makes a significant contribution to homeland security efforts—especially the sub-unified command, USCYBERCOM. Also, as mentioned in the previous chapter, the United States Coast Guard plays a direct role in CIP as the SSA for the Maritime Transportation System.[395] This extensive network of partners requires the Department of Homeland Security to maintain multiple coordination centers across the United States. Executive Order 13691[396] builds upon previous policy efforts addressing CIP.[397] It conspicuously designates the NCCIC as the primary cyber coordination center "for sharing of information related to cybersecurity risks and incidents," which connects numerous federal, state, and civilian organizations through information sharing networks like the Homeland Security Information Network for Critical Infrastructure (HSIN-CI). Ultimately, the goal of these partnerships is to mitigate risk and reduce the uncertainty associated with CIP.

Risk and uncertainty in the protection of Critical Infrastructure remains one of the single most convincing arguments for federal presence in cyberspace. This argument stems from a number of developments to industry over the last four decades. For one, many of the systems and subsystems associated with Critical Infrastructure have been in existence for decades—even centuries—but have only recently been linked through a series of networks. In many cases, these proprietary networks are attached to the Internet and are therefore vulnerable to many malicious activities that occur in cyberspace.

There are significant and convincing arguments for maintaining cyberspace as an "open, global commons of information that [allows] innovation

395 *See supra* note 157.

396 80 F.R. 9349, "Promoting Private Sector Cybersecurity Information Sharing" (February 13, 2015).

397 *See* generally EO 13636 (February 12, 2013) and PPD-21.

and rapid technological growth."[398] Pursuing these avenues is worthwhile, but they tend to be predicated on the prime objective being the maximization of innovation. These inferences often fail to recognize the exclusive Constitutional mandate for the federal provision of national defense.[399] While private industry solutions are certainly advantageous and desirable, the inextricable linkages between critical infrastructure and the security of U.S. citizens mandates a certain amount of federal presence.

One of the difficulties facing federal security provision is the fact that most major industries have connected critical services into networks that are accessible both domestically and internationally—most of them through the Internet. Many more companies are exacerbating the problem of security by replacing manual processes with automated and networked ones that have either no manual backup or no capacity for supporting service stoppage.[400] It is no more feasible to exclude the federal government from cyberspace than from security efforts in the air, space, maritime or land domains.[401]

Moreover, the 2016 Mandiant report on cybersecurity breaches reveals a significant diversification in both the location and the motivation of cyberspace attackers. Additionally, the report shows that upwards of 89% of the breaches

---

[398] *See* generally Catherine Hart, Dal Yong Jin and Andrew Feenberg, "The Insecurity of Innovation: A Critical Analysis of Cybersecurity in the United States," *International Journal of Communication* 8 (2014): 2860–78, http://ijoc.org/index.php/ijoc/article/viewFile/2774/1257.

[399] *See* generally U.S. Constitution, Art. 1 s. 8 pertaining to the powers of Congress, at least six of which deal with national security. *See* also *id.* at Art. 2 pertaining to the president's responsibility to execute the authorities of Congress. *See* also *id.* at Article 4 s. 4 requiring the federal government to protect the United States "against invasion."

[400] Water dams are just one notable example of networked critical infrastructure whose short-term failure can result in devastating environmental impacts and loss of life.

[401] This is not to suggest that the federal government should be able to operate without limitation, but it does suggest that, contrary to some critics, terms like "war" and "violence"—much like "attack," "exploit," and "defend"—are as appropriate to the realm of cyberspace as they are to the physical domains. *C.f.* DISCOURSE IS A BATTLEFIELD. Ben Kamis and Thorsten Thiel, "The Original Battle Trolls: How States Represent the Internet as a Violent Place," working paper for *ECPR General Conference* (Bordeaux, France: ECPR, 2015), 19–23, http://ecpr.eu/filestore/paperproposal/25127ed8-317f-4039-8239-b2d06e456573.pdf.

covered were distributed relatively evenly across ten industry sectors.[402] Although Mandiant is not generally the first responder to attacks on critical infrastructure, these figures illustrate the need for a holistic approach—not absent inter-title efforts—necessary to not only respond to attacks, but to perceive how and by whom they will be perpetrated in order to establish measures that prevent their occurrence.

Many of the barriers to information sharing have been addressed through previously discussed legislation like CISA and other provisions in the USA PATRIOT Act—amended and extended by the USA FREEDOM Act. Information sharing, while an essential pillar, is not the only lynch pin that is needed to enable inter-title cooperation. As will be discussed in subsequent sections, barring policy and attitude, there are significant legislative requirements in the area of budgetary responsibilities and congressional oversight. This accountability necessitates a clear delineation of operational responsibilities, which further raises questions of chain-of-command.

e. Intelligence Activities

Much of the previous conversation has already encapsulated many of the opinions and legislative challenges associated with inter-title cooperation as it applies to intelligence activities. The recommendations from the 9/11 Commission and the subsequent provisions of the USA PATRIOT Act remain the primary influences in explicitly advocating and making provision for inter-title cooperation. The U.S. armed forces (10 USC), the CIA and NSA (50 USC), the USCG (14 USC), the FBI (18 USC), and DHS (6 USC) are just a few of the beneficiaries of legislation that compels greater collaboration and information sharing between the executive departments and subordinate agencies of the federal government. Even with these mandates in place, however, there are substantial legislative ambiguities and a prolific spread of misinformation that

[402] *See* BY THE NUMBERS. Mandiant Intelligence Center, "M-Trends 2016," *Mandiant Corporation* (2016), 6, available for download at https://www2.fireeye.com/M-Trends-2016.html.

influence the course of cooperation within the IC. Negative responses to Leon Panetta's "Title 50 clarification" of the Abbottabad raid,[403] supposed legal distinctions between covert and overt activity,[404] and claims of misconduct by Congress have all unnecessarily—at least from a jurisprudence standpoint—inhibited inter-title cooperation in the area of intelligence activities.

In the case of Panetta's comments, his distinction begs the question of who is really in charge. In many ways, it can give the appearance that the armed forces are being placed at the disposal of organizations and entities that lack either the training or the authorities to direct. This attempt to distinguish operations as either exclusively "Title 10" or "Title 50" appears ignorant to the fact that the president has authorities and responsibilities under all 53 titles of the United States Code. The Secretary of Defense is delegated authorities under two of these titles—10 USC and 50 USC. Despite this longstanding delegation of authority, it continues to surprise many that a single office is capable of lawfully executing a mission or overseeing an operation under multiple title authorities.[405]

---

[403] *See* Panetta, *supra* note 361.

[404] For arguments concerning covert vs. overt legal distinctions, *see* TRANSPARENT VS. COVERT. *Supra* at Ch. 2 s. (C)(2)(b). *See* also NOTE 4. Wall, 87. "Admiral Vern Clark, former Chief of Naval Operations of the U.S. Navy, Professor John Radsan, a former assistant general counsel for the CIA, and Professor Gregory McNeal, a former Department of Justice lawyer, were asked "what is Title 10 authority?" and "what is Title 50 authority?" during a panel discussion at a law school symposium on national security law. Admiral Clark phrased the debate as one "about the line between covert and overt"" […] "yet his articulation of this concern focused on military transparency and public perceptions about the military. Professor Radsan framed the debate in terms of defined roles for the military and intelligence communities, while Professor McNeal opined that military lawyers advising special operations forces are often confused about the legal basis for their actions. National Security Symposium: *The Battle Between Congress & The Courts in the Face of an Unprecedented Global Threat: Legislation Panel: Discussion & Commentary*, 21 REGENT U.L. REV. 331, 347 (2009)."

[405] *See* NOTE 129. *Id.* at 125. "The Secretary of Defense may direct DoD personnel to carry out intelligence activities in response to national intelligence requirements, or to meet the intelligence needs of the military. When DoD personnel conduct intelligence activities in response to national intelligence requirements, they do so primarily under Title 50 authorities [50 U.S.C. § 3038] and pursuant to priorities and needs determined by the DNI [50 U.S.C. § 3024(f)]. When DoD personnel conduct intelligence activities to fulfill military intelligence requirements, those intelligence activities are conducted under Title 10 authorities, *e.g.*, [10 U.S.C. §§ 113,164], and delegated authorities from the President and Secretary of Defense; if the DoD personnel are also members of the Intelligence Community (e.g., NSA) the activities are also conducted pursuant to Title 50 authorities [50 U.S.C.§ 3038]. These military operations are also sometimes referred to as 'DoD Intelligence Related Activities' or 'Tactical Intelligence and Related Activities (TIARA).'"

Many instances where Congress has alleged inter-title misconduct can be the result of either ignorance regarding the extensive network of congressional oversight, or perhaps motivated by political attempts to further restrict presidential powers. Take, for instance, the *HPSCI Report on the Intelligence Authorization Act of 2010*. In it, the committee notes that

> clandestine military intelligence-gathering operations, even those legitimately recognized as OPE, carry the same diplomatic and national security risks as traditional intelligence-gathering activities. While the purpose of many such operations is to gather intelligence, DOD has shown a propensity to apply the OPE label where the slightest nexus of a theoretical, distant military operation might one day exist. *Consequently, these activities often escape the scrutiny of the intelligence committees, and the congressional defense committees cannot be expected to exercise oversight outside of their jurisdiction* (emphasis mine).[406]

These claims, however, show an unawareness of the fact that the armed services committees exercise regular oversight over the clandestine operations of the armed forces. Regardless of how the operation is defined, whether as OPE or covert action, it does not escape congressional oversight in one form or another.[407]

Deciding whether an action falls under the umbrella of traditional military activity or covert action is not inconsequential, however. As previously shown, there are distinct limitations on covert action and the oversight governing it represents an entirely different congressional body. In acknowledging the close relationship between these two activities, Representative David McCurdy noted in a 1991 congressional conference report that

> none of the counterintelligence activities which the Department of Defense […] reported to the intelligence committees [constituted] covert action within the meaning of this definition. [Furthermore,]

---

[406] House, *Report to Accompany H.R. 2701, 'The Intelligence Authorization Act for Fiscal Year 2010,'* 48.

[407] *See* generally Wall, 102-04.

> "traditional military activities" and "routine support" to such activities do not fall within the definition of covert action."[408]

Military intelligence activities, while authorized under 10 USC,[409] can appear identical to those intelligence activities authorized under 50 USC. In practice, however, military intelligence activities are more strictly subject to executive approval, even though they often yield identical information and are stored in the same data repositories. Realizing that there was a need to better distinguish between such activities—covert action and traditional military activities—the report suggested that four elements should be present if the intelligence activity is to be considered traditional military activity:[410]

1. Conducted by U.S. military personnel, and
2. Under the direction and control of a U.S. military commander, and
3. Preceding and related to anticipated hostilities or related to ongoing hostilities involving U.S. military forces, and
4. The U.S. role "in the overall operation is apparent or to be acknowledged publicly"

While the first two elements may be more obvious and practical, the third and fourth stipulations present some unique challenges. For cyberspace activity—as well as for traditional intelligence activities—the requirement that the activity "precede and relate to anticipated hostilities" calls into question the subjective nature of the terms. Many of the military's activities involve war-gaming and preparation for anticipated hostilities of varying degrees of likelihood. The nearness of hostilities and the validity of the threat do not prevent the U.S. military from preparing for "worst case scenarios." In this case, it would seem that traditional military activities would be given a wide berth for intelligence gathered in anticipation of hostilities. Even activities that "relate to ongoing hostilities" can

---

[408] House, *Conference Report on the Intelligence Authorization Act for Fiscal Year 1991*, H5905.

[409] 10 USC §§ 401 *et seq.*

[410] *See* Wall, 132–36.

find a variety of valid justifications depending on the extent to which the matrices of dependencies extend to ancillary variables.[411]

The fourth stipulation can hardly be applied in a consistent manner since there are a number of military operations—both in cyberspace and the physical domains—that are intended to be concealed and not acknowledged publicly. It would seem then, that while a lack of public acknowledgement would not exclude the activity from being traditional military activity, the presence of a public acknowledgement would exclude the presence of a covert action.[412] Returning again to the Abbottabad raid, this would seem to indicate that the operation was more of a traditional military activity than a covert action. To label it as either "Title 10" or "Title 50," however, is overly simplistic and, as with many oversimplified conclusions on inter-title cooperation, it fails to account for many of the fiscal and oversight requirements associated with the operation.

These arguments extend beyond just 10 USC and 50 USC. This line of reasoning applies to Title 6 and Title 10 interactions which require that the Secretaries of the DOD and DHS "shall provide personnel, equipment, and facilities in order to increase interdepartmental collaboration" that will "leverage the expertise of each individual Department and [avoid duplication of effort]."[413] This mandate necessarily draws in the Coast Guard (14 USC) while considerations for the FBI still primarily fall under 50 USC—as delineated by the president in EO 12333. This special attention given to intelligence activities reveals critical arguments that are no less significant in cyberspace, where the activities characterizing intelligence gathering are, in some cases, indistinguishable from traditional military activities. Under an examination of

411 Ibid.

412 Ibid.

413 Pub. L. 112–81, div. A, title X, § 1090, which concerns "Cybersecurity Collaboration Between the Department of Defense and the Department of Homeland Security."

general legisprudence,[414] it is reasonable to propose that whether the separation results from policy or legislation, they should remain subject to constant reexamination and be regularly adjusted to preserve the fundamental rights of citizens while also effectively addressing changes in environmental, social, technological, economic, and geopolitical contexts.[415]

B. INTER-TITLE CYBERSPACE OPERATIONS

Central to the enablement of inter-title operations in cyberspace is the need for balance. In keeping with the purpose of the United States Code, it is clear that there remains a distinct and pronounced need for an assured cyber-capability and the reliability of an effective cyber-response. Reduced timelines associated with cyberspace and the potentially devastating effects of security patches underpin growing demands for increased secrecy and policies that enable more-rapid decision making. On the other hand, there remains the fundamental requirement to ensure that frameworks exist for facilitating appropriate oversight and compliance, and ultimately for ensuring that government powers remain subject to the rule of law.

Many critics see in this process an erosion of the U.S. legal framework as it is continually reinterpreted in the context of expanded cyberspace efforts and growing concerns for increased national security. Some of these criticisms rightly point out that the legal difficulties presented by cyberspace are not simply restricted to geographic concerns or the "indeterminate collateral consequences" associated with cyber effects.[416] Characterization of threats, categorization of

---

[414] *See* generally Luc Wintgens, ed., *Legisprudence: New Theoretical Approach to Legislation* (Portland, OR: Hart, 2002). A phrase coined by Luc Wintgens as early as 1992. Rather than focusing on the *application* of the law by judicial authorities, legisprudence expands the context to include studies on the *creation* of the law by legislators.

[415] *See* generally W. R. Stahel, "The Service Economy: 'Wealth Without Resource Consumption'?," *Philosophical Transactions: Mathematical, Physical and Engineering Sciences* 355, no. 1728 (July, 1997): 1309–20, http://www.jstor.org/stable/54751. Adapted from Stahel's "five pillars of sustainability."

[416] *See* generally Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," 580–83.

activities, and even the burdens of *ex ante* determinations that are associated with employing cyber-munitions are all contributors that increase the number of obstacles and compound the complexity facing decision makers and legislators alike.[417] In this case, a basic understanding of the strategic, organizational, and technical challenges of cyberspace should expose much of the misinformation currently in circulation.

Dissenting claims are often paired with many of the misleading arguments identified previously[418] and assert that current methods for strategic planning and execution are not possible within the context of cyberspace. Unique challenges from cyberspace are undeniable, but a strategic overhaul based on unsubstantiated claims of incompatibility tends toward overreaction. The 2015 National Security Strategy for example, calls for increased pressure against terrorist groups and their affiliates.[419] From a cyberspace perspective, the idea of combatting malicious hacking conducted by terrorists and disrupting their use of social media[420] is not so dissimilar from the kinetic strikes conducted against terrorist training compounds and Information Operations (IO) campaigns that achieve similar counterinformation objectives in the physical domain.

This brief example illuminates an important aspect of cyberspace operations, which is that, while they may require effects to be delivered between two network nodes, their activities are folded into an overall strategy that involves traditional military responses in the Land, Maritime, Air, and Space domains.[421]

Though not directly related to inter-title cooperation, an often disruptive source of misinformation is found in the perceived social gap between the sorts

---

[417] Ibid.

[418] *Supra* at Ch. 2 s. (C)(2).

[419] *See supra* note 132.

[420] E.W., "Should Twitter Block Islamic Snuff Videos?," *Economist*, Aug 21, 2014, http://www.economist.com/blogs/democracyinamerica/2014/08/twitter-terror-and-free-speech.

[421] *See* generally Brett Williams, "Cyberspace: What Is It, Where Is It and Who Cares?" *Armed Forces Journal*, March 13, 2014, http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares.

of individuals who are suited to the organization of the federal government and those whose expertise is in cyberspace—the presumption being that the two are generally incompatible. Cultural stereotypes have led to the idea that those most suited for cyberspace are incapable of being effective within a traditional chain of command and, in the case of the military, will be encumbered by a uniform, and are unlikely to meet necessary physical fitness standards.[422] Too many members of the military harbor a defeatist attitude about the government's—particularly the military's—ability to attract talented individuals who are presumed to be the sort of "anti-establishment loners" or "geeks" who are only interested in the more lucrative jobs offered by the civilian sector. This idea that the best cyberspace operators are overweight, opposed to discipline, and consumed with online video game—played from their parents' basement—is hardly an accurate depiction of modern-day cyberspace actors. Instead, modern studies are increasingly showing that the nature of cyberspace actors and hackers is more complex than previously imagined and tends to be present in an assortment of self-taught and highly trained individuals.[423] As subsequent generations receive increased exposure to information technology at earlier ages, the recruiting pool will inevitably increase and aptitude should emerge from a variety of groups within society.

In a similar vein, the sheer size and complexity of cyberspace become too daunting to comprehend and incorporate. As such, the highly technical nature of cyberspace has been deemed an insurmountable problem with its composition of not only logical and physical components, but of endless cyber personas that are an amalgam of people, groups, and sometimes pets. This can create any number of complications, which in turn may prevent executing operations under clear

[422] *See* THINKING AHEAD. James Stavridis and David Weinstein, "Time for a US Cyber Force," *Proceedings* 140, no. 1 (January 2014): 44.

[423] *See* generally Timo Gnambs, "What Makes a Computer Wiz? Linking Personality Traits and Programming Aptitude," *Journal of Research in Personality* 58 (October 2015): 31–34. *See* also, Jim Romeo, "The Hacker Beside You," *Transaction World Magazine*, May 1, 2014, www.transactionworld.net/articles/2014/may/cover-story.html. *See* also, Emma Sturgis, "10 Myths About Hackers (That Are Totally False)," *Nerd Like You*, September 8, 2015, http://www.nerdlikeyou.com/10-myths-about-hackers-that-are-totally-false.

authorities or consistent Rules of Engagement (ROE). The complicated answer to this will be addressed by the proposed framework, but the complexities associated with comprehending the legislative authorities for cyberspace operations is significantly more encumbering when compared with the stability of its architecture and protocols.

Another key vantage point that presents cyberspace in a more accessible manner is the priority to view it primarily as a domain and not an arrangement of networked systems. Analogies are very useful in analyzing policy and strategy situations, but they tend to be a double-edged sword when associated with cyberspace.[424] The diverse and numerous arguments over appropriate analogues might seem to suggest that suitable analogies do not exist for cyberspace. More accurately, however, it is unlikely that a single analogy can completely convey the nature of cyberspace. Furthermore, this limitation on analogy applies to every domain. While earlier discussions revealed deficiencies in establishing a complete physical-to-cyberspace equivalence,[425] the current discussions are looking at the problem from a broader perspective. For example, it was previously stated that there is doubt as to whether or not an order to disperse can be issued by the president for cyberspace operations.[426] The absence of a direct equivalence, however, does not prevent the Executive from responding to threats—especially those against individual states. If the environment of cyberspace is capable of supporting the sort of destruction and

[424] For CYBERSPACE WARFARE ANALOGIES, *see* generally Sean Lawson, "Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States," *First Monday* 17, no. 7 (July, 2012) http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270. For CYBERSPACE BOUNDARY ANALOGIES, *see* generally Duncan B. Hollis, "Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?," in *Cyber War: Law and Ethics for Virtual Conflicts*, eds. Jens David Ohlin, Claire Finkelstein and Kevin Govern (Oxford: Oxford University Press, 2015), 129–74. "Law-by-analogy" provides a way to replicate earlier laws in Cyberspace, but becomes increasingly difficult in situations where there is no suitable analogue. Analogies are useful in some instances, but at some point cyberspace requires a more crafted approach to delineating boundaries. For "CYBERSPACE AS PLACE" ANALOGIES *see* generally Kathleen K. Olsen, "Cyberspace as Place and the Limits of Metaphor," *Convergence: The Journal of Research into New Media Technologies* 11, no. 1 (Spring 2005): 10–18, http://www.andredeak.com.br/pdf/cyberspace.pdf.

[425] *See* INTERNATIONAL VS. DOMESTIC. *Supra* at Ch. 2 s. (C)(2)(c).

[426] *Supra* note 176.

havoc that is analogous to an insurrection in the physical domains, then its actors and activities can be made subject to relevant statutes.

To state this problem more succinctly, limited aspects of cyberspace can be subjected to analogy in constructive ways. Furthermore, while it is unlikely that a single analogy can completely capture the whole of the cyberspace domain, it is equally unlikely that any single analogy could fully encapsulate the aspects for any of the physical domains. In the case of space, there is a vastness and overlap with the air domain that allows territorial encroachment that is not shared in the other physical domains. Furthermore, its unique physical characteristics share traits with the maritime domain that are distinct from the air and land domain.[427] Therefore, it is likely that the misapplication of analogy has more to do with its undisciplined approach than with a lack of suitability. In each case, however, the importance of the domain is linked to its broad use across a myriad of disciplines that include domestic and international use in areas like the economy, information, civilian, and government. In addition to providing support for these individuals and interests, each of these domains—no less cyberspace—are home to a host of criminals and criminal activity.

In this way, cyberspace has much in common with the complex and multi-faceted physical domains, and especially with the maritime and space domains, which are largely associated with freedom of use and generally characterized as a "global commons."[428] This idea of shared space inevitably leads to the presence of numerous stakeholders—federal stakeholders in the case of the U.S. government—and lends itself toward an environment where mutual support is often a natural byproduct of the coordination necessary among the various agencies and organizations operating there. This being said, the varying levels of

---

[427] *See* generally Elizabeth Howell, "The Ocean Is A Lot Like Outer Space," *Universe Today: Space and Astronomy News,* January 23, 2013, http://www.universetoday.com/99593/the-ocean-is-a-lot-like-outer-space.

[428] *See* generally Mark Barrett, Dick Bedford, Elizabeth Skinner and Eva Vergles, *Assured Access to The Global Commons* (Norfolk, VA: NATO Headquarters, 2011), http://www.act.nato.int/images/stories/events/2010/gc/aagc_finalreport.pdf.

friction that cyberspace experiences with other domains does not make it incapable of lawfully appropriating relevant federal authorities. Already a resounding theme of this paper, the following section will show that the United States Code does not present an ethical contradiction for the management and use of cyberspace through inter-title cooperation.

IV. FRAMEWORK FOR INTER-TITLE OPERATIONS

Previous discussions have been primarily concerned with dispelling misinformation about cyberspace and inter-title operations. A number of particularly negative conclusions purporting to be legal prohibitions have been exposed to be merely policy matters masquerading as legal concerns. Some of these alleged restrictions stem from political maneuvering amidst the perpetual struggle for greater control that exists primarily between the executive and legislative branches. More still are the result of national concerns over the extent of power and control bestowed upon the U.S. government as many are prone to cite potential damage to the United States' reputation amongst its international partners. Some of these concerns are easily dismissed or else addressed through new or revised policy. Other concerns are considerable and go to the very heart of how Americans see themselves and how they want to be perceived. Practically, however, these desires find very little footing in available legislation.

As noted previously, philosophical concerns over the United States Code generally do not address legislative implementation and authorities. Having scrutinized many of these concerns under the *lex scripta* of domestic law, it is now essential to turn the focus to constructing the framework under which cyberspace operations can be planned and executed. Throughout the preceding sections, legitimate legal concerns have generally fallen into three broad categories: oversight and compliance, fiscal controls, and statutory authority. The following sections will address these in greater depth, which will result in a simplified framework for understanding the legal requirements associated with planning and executing inter-title operations.

A. OVERSIGHT AND COMPLIANCE

The United States Congress has no explicit right to oversight and compliance through any stipulation in the U.S. Constitution. It seems however, that the constitutional implication for congressional oversight has always been

assumed by its founders and has thus been firmly established since the country's founding. Congress largely exercises oversight through two primary means. The first is through the standing committee system. Reports detailing expenses associated with the latest in military advancements will often highlight congressional comments originating from the House Armed Services Committee (HASC) or the Senate Armed Services Committee (SASC). These committees are specifically responsible for overseeing military activities (10 USC and 32 USC) as they relate to "common defense"[429] and ensuring the lawful employment of authorities under standing policy and in accordance with applicable legislation.[430] The constitutional authority granted to the president as the executive power and Commander in Chief[431] restricts Congress from exercising control over the ways and means by which the president employs these forces. Instead, the House and Senate Appropriations Committees are only able to limit which budgetary line items will be funded—vis-à-vis the annual Department of Defense Appropriations Act. This level of control is significant but not nearly as extensive as those that are afforded to Congress as they oversee intelligence activities.

For intelligence activities (50 USC), the Senate Select Committee on Intelligence (SSCI) and Permanent Select Committee on Intelligence of the House of Representatives (HPSCI) exercise significant oversight.[432] Statutes require intelligence committees to be kept "fully and currently informed of all intelligence activities, other than covert action."[433] The subset of intelligence activities known as "covert action"[434] requires presidential authorization and

---

[429] U.S. Congress, Senate, Committee on Rules and Administration, *Standing Rules of the Senate*, 113th Cong., 1st sess., 2013, S. Doc. 113-18, Rule XXV s. (1)(c)(1)(2), https://www.gpo.gov/fdsys/pkg/CDOC-113sdoc18/pdf/CDOC-113sdoc18.pdf.

[430] *Id.* at s. (1)(c)(2)

[431] Pursuant to U.S. Constitution, Art. 2, ss. 1,2.

[432] Pursuant to 50 USC §§ 3091 *et seq.*

[433] Pursuant to *id.* at § 3092(a)(1).

[434] As defined in *id.* at § 3093(e).

notification to the relevant committees "as soon as possible after such approval and *before* the initiation of the covert action."[435] By default, covert actions do not have appropriated funds and may not receive funding until a presidential finding has been submitted to the appropriate committees, with the HPSCI exercising additional scrutiny beyond their Senate counterpart.

Although the statutes of this section maintain that the oversight stipulations are not to be construed as "requiring the approval of the [committees]" to initiate intelligence activities, the House rules governing the conduct and jurisdiction of the committees stipulate that the HPSCI are additionally authorized to review the "sources and methods"[436] associated with intelligence activities within their jurisdiction.[437] Reporting requirements alone may not halt the intelligence activities of executive agencies, but when subjected to the broad scrutiny of the intelligence committees and approval by relevant appropriations committees, it is clear that the legislation indeed does make provision for granting Congress some significant control in managing the execution of Title 50 authorities.

While intelligence activities may appear to have a number of hurdles to successfully employing them in inter-title activities, the Department of Homeland Security likely presents the greatest challenge. The oversight is so complex that 6 USC simply states that throughout the federal statute,

> the term "appropriate congressional committee" means any committee of the House of Representatives or the Senate having

[435] Pursuant to *id.* at § 3093(c)(1)

[436] *See* U.S. Congress, House, Committee on Rules, *Rules of the House of Representatives of the United States One Hundred Thirteenth Congress*, 113th Cong., 2nd sess., 2015, H. Doc. 113-181, § 744 Rule X s. (3)(m), https://www.gpo.gov/fdsys/pkg/HMAN-114/pdf/HMAN-114.pdf. This review of "sources and methods" is a further source of tension with the Executive branch and other committees like the Committee on Appropriations.

[437] *See id.* at s. 12(a). For FISA related activity, HPSCI shares jurisdiction with House Committee on the Judiciary (HJC). *See* also *id.* at ss. 11(b)(1)(B),11(b)(1)(D)(ii). The HPSCI claims jurisdiction over activities and requests for appropriations dealing with "Intelligence and intelligence-related activities of all other departments and agencies of the Government, including the tactical intelligence and intelligence-related activities of the Department of Defense." This would require a shared jurisdiction with the HASC as it pertains to military intelligence.

> legislative or oversight jurisdiction under the Rules of the House of Representatives or the Senate, respectively, over the matter concerned.[438]

This process and the ensuing debates over inter-title cooperation would be enormously simplified if Congress were to align its congressional committees to the relevant statutory authorities.[439] Frequent attempts have been made to depict committee involvement in homeland security in a way that either clarifies congressional oversight over DHS as it pertains to Title 6 and Title 14, or else in a way that demonstrates the extent of its dysfunction.[440] For the present purposes of constructing a framework, only four of the more than 30 relevant oversight committees will be addressed. This small sample size should not adversely impact the framework since the inclusion of these four still demonstrates the need for operational planners to identify and notify the correct congressional body as relevant aspects of the operation may pertain to homeland security operations. Numerous and significant research has delved into the spider's web of oversight committees that influence homeland security,[441] and while the oversight structure has yet to be optimized, it remains suitable for the purposes of supporting inter-title operations.

The first two committees reside within the Senate. They are the Senate Committee on Homeland Security and Governmental Affairs (HSGAC) and the

---

[438] 6 USC § 101(2)

[439] Wall, 107.

[440] *See* APPENDIX A. Center for Strategic and International Studies (CSIS) and Business Executives for National Security (BENS), *Untangling the Web: Congressional Oversight and the Department of Homeland Security* (Washington DC: CSIS and BENS, 2004) http://csis.org/files/attachments/041210_dhs_whitepaper.pdf. *See* also Task Force on Streamlining and Consolidating Congressional Oversight of the U.S. Department of Homeland Security (DHS Congressional Oversight Task Force), *Streamlining and Consolidating Congressional Oversight of the U.S. Department of Homeland Security*, (Washington DC: Aspen Institute , 2013): 11, http://www.aspeninstitute.org/sites/default/files/content/docs/pubs/Sunnylands%20report%2009-11-13.pdf.

[441] *See* generally Ibid. *See* also David P. O'Leary, "Beyond Measure: New Approaches to Analyzing Congressional Oversight of Homeland Security," (master's thesis, Naval Postgraduate School, 2015). *See* also Peter J. May, Ashley E. Jochim and Joshua Sapotichne, "Constructing Homeland Security: An Anemic Policy Regime," *Policy Studies Journal* 39, no. 2 (2011): 285–307, doi: 10.1111/j.1541-0072.2011.00408.x. *See* also Tapan Sen, "Congressional Oversight of Homeland Security: Help or Hindrance?," (master's thesis, Naval Postgraduate School, 2012).

Senate Commerce, Science, and Transportation Committee (CS&T). The HSGAC has oversight over all major functions of DHS with the exception of the USCG, immigration services, and the USSS[442] while the CS&T has oversight over the USCG and coastal zone management, to include inland waterways.[443]

The next two committees are the House Committee on Homeland Security (CHS) and the House Transportation and Infrastructure Committee (T&I). The obvious counterpart to the HSGAC, the House's CHS oversees large parts of the DHS mission as it broadly pertains to Title 6 authorities. Its jurisdiction begins with the organizational structure that supports homeland security operations and covers most major DHS functions like border security, customs, threat notifications, domestic preparedness, and counterterrorism.[444] Furthermore, one of the special oversight functions of the CHS is to oversee all interagency activity involving DHS,[445] which would naturally extend to inter-title operations. The T&I is the counterpart to the CS&T in that it provides oversight for Coast Guard activities as well as coastal regions and inland waterways.[446]

The final two congressional committees considered for the framework are generally responsible for providing oversight to Title 18 and Title 28 authorities. These congressional bodies are the House Judiciary Committee (HJC)[447] and the Senate Judiciary Committee (SJC).[448] The overlap between criminal and judicial procedure and other title authorities requires the judiciary committees to participate in a significant number of other jurisdictions—6 USC, 14 USC, and 50 USC being the most notable examples.

---

[442] *See* APPENDIX. Senate Committee on Rules, 73–76. Exception is pursuant to S. Res. 445, s. 101(b)(1), (October 9, 2004).

[443] *Id.* at Rule XXV s. (1)(f)(1)

[444] *See* House Committee on Rules, Rule X § 723a(1)(j).

[445] *Id.* at Rule X § 744 (3)(g)(1)

[446] *Id.* at Rule X § 739 (1)(r)

[447] *Id.* at Rule X § 729 (1)(l)

[448] Senate Committee on Rules, Rule XXV s. 101(m).

Table 1 represents the first major step in clarifying oversight for planners who are preparing for inter-title operations. This consolidated view of congressional oversight committees forms one of the strongest arguments for inter-title operations. In many ways, the overlapping jurisdictions within the statutory framework mirrors the overlapping jurisdictions within the congressional oversight structure. Having already identified numerous areas of overlap in authorities throughout the previous sections, it is critical to identify congressional committee overlap in order for relevant Senate and House oversight committees and sub-committees to ensure that operations comply with statutory limitations and reporting requirements. This may appear an insurmountable task, but it is important to recognize that fulfilling the oversight stipulations of the committees can be effected through already established channels. Congress can establish these reporting requirements by codifying them under the relevant U.S. title code, or by incorporating them into appropriations and authorization bills. One notable example of this is found in the Title 6 section on "Information and Analysis and Infrastructure Protection,"[449] which authorizes inter-title cooperation and has initial—and codified—reporting requirements[450] as well as additional reporting requirements identified in annual legislation.[451]

[449] 6 USC § 121

[450] *Id.* at § 121(d)(25).

[451] Pub. L. 111-259, title III, §336, e.g., the Intelligence Authorization Act of 2010, which provides statutes pertaining to cybersecurity oversight.

Table 1. Title Authority and Its Relation to Congressional Oversight

Title Authority	Oversight Body
6 USC	HSGAC/CHS (CS&T/T&I)
10/32 USC	SASC/HASC*
14 USC	CS&T/T&I (HSGAC/CHS)
18/28 USC	SJC/HJC
50 USC	SSCI/HPSCI†
SAD	State Committee

* Under executive control of the Commander in Chief, activities pursuant to relevant authorities are, in general, only limited by the president. †Current structures for congressional oversight make congressional approval, in general, a necessity for authorizing intelligence activities—to include covert activity.

This table of oversight can facilitate enabling inter-title cyberspace operations by ensuring that the proper congressional oversight committees are informed of the efforts of each agency and organization involved in the operation. As planning is conducted, federal operators must remain cognizant of how their participation—assuming it is statutorily authorized—translates to reporting requirements for pertinent congressional committees. In some cases, the oversight requirements are fulfilled subsequent to an operation, but in other cases—as is the case with covert action and previously unapproved intelligence activities—it must be done prior to conducting the operation. In most cases, this can hardly be done without communicating the full extent of the inter-title cooperation including relevant stages the ultimate objectives of the operation. To accomplish this, operational planners would require a quorum of all pertinent committees to be present to convey the extent of activities and the role to be performed by each organization and agency.

Fulfilling oversight requirements in this scenario is hardly plausible for upward of seven title authorities and 40 or more congressional committees. Instead, as is often the case with jurisdictional overlap, there is a process by

which reporting is sequentially passed from one congressional committee to the other. In some cases, legislation has streamlined the reporting process. In terms of cybersecurity, relevant departments are statutorily required to choose a lead organization to coordinate required reporting to Congress and the president.[452] This scarcely eases the burden of congressional oversight, but at the very least, it demonstrates the possibility for consolidated reporting from organizations operating under distinct title authorities. Where consolidated reporting is not possible or prohibited, there is likely a benefit in vying to be the final committee to scrutinize the inter-title operation after all adjustments have been made and recommendations incorporated from previous committees. Recommendations for a congressional committee succession plan will be outlined under discussions in the final section of this chapter.

B. FISCAL REQUIREMENTS

Fulfilling the requirements of congressional oversight does not ultimately overcome the legislative hurdles associated with inter-title cooperation. Though there is a fiscal aspect to the oversight and compliance exercised by Congress over activities conducted under the United States Code, fiscal concerns are vetted through avenues that, in many cases, are entirely independent of the relevant congressional oversight committees. In some cases, this stems from the fact that once funds are assigned, there is a certain amount of discretion over how and under what conditions they can be used.

In this, there is an inherent and sometimes explicit responsibility for cooperating agencies and organizations to share costs associated with executing their joint mission. In turn, this requires determinations as to what constitutes the fair share of each participating authority. These determinations are easier in cases involving cooperative research and development efforts between two organizations—like those statutes that govern Coast Guard and Navy contracting

[452] Pursuant to *id.* at, § 336(b)(3).

efforts.[453] It becomes significantly more complicated in inter-title operations where one agency's role may be more central to the operation than those of supporting organizations. In the case of funds governing intelligence, this is less complicated since the task is generally delegated to the ODNI who is given a significant amount of statutory discretion in expending appropriated funds.[454] Other provisions for intelligence allow the president to exercise discretion over non-appropriated funds in support of activities that have not been explicitly denied by congressional oversight committees.[455] The expenditure of these types of funds usually comes with additional statutory reporting if they are not expended under previously approved activities. While the administrative challenge associated with this task is immense, it is important to recognize that, with few exceptions, there is no statutory prohibition against making this determination.

Along similar lines, some statutes allow for the unique capabilities of one organization to be utilized by another. It is helpful to imagine a proverbial pooling of federal assets. Agencies that are inhibited in exercising their authorities by other-than-statutory deficiencies may, in some cases, employ federal resources that are under the patronage of another agency or organization. Depending on the complexity of this resource or the requesting agency's resident level of expertise, there may be additional requirements to employ operators who can effectively respond to that agency's operational command authorities. In other cases, the agency may just require access. In any case, there is a need to identify this type of "loaning" behavior since it requires reimbursement throughout many relevant statutes.

Title 6, for example envisions the corporate employment of effort and resources by the State Department, CIA, FBI, NSA, NGA, DIA, and "any other

---

[453] 14 USC § 566

[454] *See* generally, 50 USC § 3024(c). Fair share between intelligence activities is at the discretion of the Director of National Intelligence so long as it falls under the National Intelligence Program activities.

[455] 50 USC § 3094.

agency of the Federal Government that the President considers appropriate" in creating a consolidated intelligence picture to support infrastructure protection.[456] This same statutory section authorizes cybersecurity collaboration between the DOD and DHS and explicitly states that "the Secretary of Defense and the Secretary of Homeland Security shall provide personnel, equipment, and facilities in order to increase interdepartmental collaboration."[457] There are further stipulations that prevent these provisions from being used to circumvent statutory prohibitions,[458] but the salient point in all of this is that the multitude of interactions will incur costs that will need to be shared between the agencies and organizations involved in the operation.

Another fiscal consideration concerns the appropriations committees that reside in the House and Senate. These committees are less concerned with compliance as it concerns the intent of relevant statutes. As previously discussed, the vast expanse of standing and select committees and subcommittees throughout the Congress are responsible for compliance. Instead, appropriations committees are concerned with linking specific amounts of money in the federal budget to specific statutory requirements as codified in the U.S.C. and various legislation.[459] As such, the efforts of the appropriations process manifest themselves through three distinct products. The first is seen in regular appropriations bills that provide funding for the associated fiscal year. As

---

[456] 6 USC § 121(f)(2)

[457] Pursuant to relevant statutes contained in the National Defense Authorization Act of 2012 (Pub. L. 112-81).

[458] For example, the creation of any new cybersecurity initiatives is required to be reported by the president to Congress within 30 days of commencement of operations in a report that must justify the *legal basis* for such program (pursuant to 18 USC § 2511(2)(a)(ii)(B)). *See* also POSSE COMITATUS ACT (18 USC § 1385). *Supra* at Ch. 2 s. (C)(4)(c).

[459] *See* SUMMARY. U.S. Library of Congress, Congressional Research Service, *The Congressional Appropriations Process: An Introduction*, by Jessica Tollestrup, R42388 (2014) http://www.senate.gov/CRSReports/crs-publish.cfm?pid=%260BL%2BP%3C%3B3%0A. "Congress annually considers several appropriations measures, which provide discretionary funding for numerous activities—for example, national defense, education, and homeland security—as well as general government operations. Congress has developed certain rules and practices for the consideration of appropriations measures, referred to as the congressional appropriations process."

with the Consolidated Appropriations Bill of 2016,[460] these bills are sometimes complicated by additional statutory inclusions that are unrelated to fiscal distributions.[461] The next comes in the form of continuing resolutions—more notable examples include bills to avoid "government shut-downs." The third is found in supplemental appropriations bills, which generally provide "additional funding for selected activities over and above the amount provided through annual or continuing appropriations."[462] A salient point to this is that each of these pieces of legislation outline terms under which funds are to be used and possible additional reporting requirements associated with their expenditure.

Congressional approval of financing is a complicated but necessary requirement in the process of establishing an inter-title framework. This is because the budget that Congress passes—as approved by the president—delineates how much money will be expended under each title authority. These line items can be extremely specific. Take for instance the Intelligence Authorization Act for 2015,[463] which allocates $507,400,000 to the ODNI "to be appropriated for the Intelligence Community Management Account."[464] As such, determining fair share becomes an integral part of planning and executing inter-title operations.

Determination of fair share is not a new concept for federal organizations. The Department of Transportation "ensures effective cooperation between the DOD, Department of Transportation (DOT), and State DOTs in matters pertaining to defense use of public highways." Governing instructions like the Defense Transportation Regulation (DTR) and funding lines—like those governing federal-aid funds to the interstate system or Defense Access Road funds—are prevalent

---

460 Pub. L. 114-113.

461 *See supra* at Ch. 2 s. (C)(4)(e).

462 CRS, *The Congressional Appropriations Process: An Introduction*, 15.

463 Pub. L. 113-293

464 *Id.* at s. 104(a).

throughout executive departments and subordinate agencies. One area requiring significant consideration is unsurprisingly in the domain of cyberspace.

Most operations in cyberspace require the use of techniques or munitions that may require a significant amount of capital to develop[465] and have a limited capability for reuse. This complication is not trivial because in addition to being difficult, determining fair share may become highly contentious between those agencies that are vying for use of limited capabilities. USCYBERCOM, in conjunction with DHS, may be the best suited for making fair share determination on shared systems and for the use and sustainment of equipment, personnel, and munitions.[466] Ultimately, however, this becomes a matter for policy makers and is not beyond the scope of legislation to authorize. Table 2 represents the minimum fiscal considerations needed to make inter-title determinations in support of cooperative cyberspace operations.

[465] Aliya Sternstein, "$460M CYBERCOM Contract Will Create Digital Munitions," *Defense One*, October 5, 2015, http://www.defenseone.com/technology/2015/10/460m-cybercom-contract-will-create-digital-munitions/122556.

[466] In the case of cyber-munitions, if prices associated with each munition are paid for under authorized funds, then the use of that munition may accomplish one organization's goals at the expense of another. Another consideration may allow the pooling of funds to create an available armory of cyber-munitions that teams may utilize when necessary. This, however, might favor more active agencies like, presumably, the DHS and DOD. If cyber munitions are developed in isolation then disparities in training and skill-level could put some organizations at a significant disadvantage. This may also lead to fiscal excesses as this option leaves open the possibility for cyber-munitions to be developed in parallel. *A fortiori*, the increased cost would not prevent the munition's loss to all entities once it is used by a single organization.

Table 2. Title Authority and Its Relation to Fiscal Requirements

Title Authority	Fiscal Responsibility		
	Funds	Personnel	Reimbursement
6 USC			
10/32 USC			
14 USC			
18/28 USC			
50 USC			
SAD			

Under this format, planners can determine relevant fiscal allowances and prohibitions, and assign funding lines, dollar amounts, or share percentages.

The entries in this table are blank and must be filled in by the planners, which can be done in a number of ways. For simpler operations, the spaces can be used to more thoroughly characterize the assets being made available by each participating organization (i.e., fiscal allocations, funding lines, number, and skills of personnel needed, etc.). For operations that are large, complicated, or contain multiple stages, these boxes can contain references to more thorough fiscal assessment.

Fiscal considerations may be the most difficult hurdle to inter-title cooperation, but is not beyond the grasp of planners and administrative staffs. In many cases, the statutory requirements go unutilized because of overly restrictive policy or an absence of any documentation on the type of cooperation being requested. In the short-term, these issues can primarily be solved through memoranda of agreement, but with the dynamics of cyberspace, there may be a need for a more comprehensive policy to address the difficulty associated with making fiscal determinations.

C. RESPONSIBILITY AND COMMAND AUTHORITY

One area that has yet to be explicitly discussed is that of responsibility and command authority. The doctrine of the U.S. military approaches the complexity of operations by ensuring that their operators are able to derive their direction from a single source. The essence of this is seen in operational planning efforts that seek both "unity of command" and "unity of effort."[467] This is not strictly a military principle, however, nor is it a concern that only has cognizance in the Executive branch. The successes and failures of U.S. operations—both domestically and abroad—have led congressional legislators to create statutory requirements in the areas of responsibilities and command authority.

Legislation is keen to outline the primary missions and responsibilities of each department. The DHS for example has the primary mission of preventing terrorist attacks against the United States and for investigating and prosecuting terrorism.[468] In the latter case, jurisdictional conflicts are alleviated by clarification that this authority is not exclusively vested in DHS, "but rather in Federal, State, and local law enforcement agencies with jurisdiction over the [terrorist] acts in question."[469] This clarification in itself, however, presents a complication in that there is a recognition of competing and overlapping jurisdictions. The Executive branch has responded to these statutory ambiguities by developing the concept of the Lead Federal Agency (LFA) where there is significant overlap between authorities. The DOJ, for example, is the LFA for domestic crisis management and, in response to potential threats, is required to coordinate with federal, state and local agencies to develop procedures and guidelines.

---

[467] *See* generally Chairman, U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington DC: CJCS, August 11, 2011): xvi. *See* also *id.*, *Doctrine for the Armed Forces of the United States*, Joint Publication 1-0 (Washington DC: CJCS, March 25, 2013): xxiii. "Unity of command is strengthened through adherence to the following C2 tenets: clearly defined authorities, roles, and relationships; mission command; information management and knowledge sharing; communication; timely decision making; coordination mechanisms; battle rhythm discipline; responsive, dependable, and interoperable support systems; situational awareness; and mutual trust."

[468] 6 USC § 111(b)

[469] *Id.* at § 111(b)(2).

The designation of an LFA, however, does not necessarily lead to unity of command and unity of effort. In the case of Hurricane Katrina relief efforts, the LFA was designated as FEMA, but relief efforts demanded the direction of federal law enforcement efforts, a task for which FEMA is not suited--nor does it have sufficient statutory authority to direct the employment of armed forces in certain tasks. Many of the statutory restrictions that led to unsuccessful response efforts in the wake of Hurricane Katrina were amended in the National Defense Authorization act of 2010, which eliminated many of the mutually exclusive aspects of Title-10/Title-32 as they pertain to Chain of Command and "allowed specially designated National Guard officers to command forces in both a Title 10 and Title 32—designated as a Dual Status Commanders."[470]

Support roles, by contrast, neither require active participation, nor preclude it. Support to inter-title operations as provided by DOD in the form of equipment and facilities is an example of a passive support role that is founded in statutory authority.[471] Authorities for passive support are primarily designed to provide necessary training, equipment, facilities, and personnel. When using passive support, consent from the supporting agency becomes a primary consideration since a lack of consent may pose problems in the area of funding or even preclude use of the support altogether. Conversely, in areas where active roles are authorized, there may be statutory mandates that require assistance or leave it as optional—as is typically the case when the support does not provide a unique capability to the operation or when its use adversely affects the supporting agencies ability to fulfill their primary mission requirements.[472] Ideally, leveraging the title code is about meeting the threshold for conducting

[470] U.S. National Guard, "NGAUS Fact Sheet: Understanding the Guard's Duty Status," accessed March 14, 2016, http://www.ngaus.org/sites/default/files/Guard%20 Statues.pdf.

[471] *See* generally 10 USC § 374.

[472] e.g., *id.* at § 376 as it pertains to military support to law enforcement to the extent that the "provision of any such support does not adversely affect the military preparedness of the United States." *See* also 6 USC § 148(e)(1) as it pertains to the NCCIC. In general, the NCCIC is responsible for coordinating cybersecurity responses "to the extent practicable" and the rendering of its services to not constitute a "right or benefit."

action and the rules of evidence that apply in order to prosecute targets. This is threshold is generally for domestic responses than it is for foreign responses.

Extensive legislation is already in place that allows for cooperation between agencies supporting various intelligence requirements, in support of counterterrorism, support to CIP, and in support of emergency response efforts.[473] Even in these cases, however, there remains the possibility for operators to confuse the primary objective with their own organizational goals and to incorrectly assign lead authorities to the overall operation. Examples from Katrina relief operations demonstrated as much and cyberspace jurisdictions are no less convoluted.

Many pertinent changes to cyberspace legislation have provided a modest remedy for many of these issues. A large portion of the policy interpretations for this legislation is currently classified and this thesis will not venture to comment on any "leaked" classified material that has yet to be declassified, regardless of the possibility of its presence in the private sector. While possibly helpful to discussion, any analysis of policy and procedure remains arbitrary. For the purposes of the framework, it will suffice to acknowledge that operations will require the designation of a lead authority or lead agency to provide foundational statutory authority to the breadth of the operation. Activities may draw on the authorities of other agencies in order to accomplish the operational objectives.

As mentioned earlier, The Secretary of Defense possesses authorities under both Title 10 and Title 50. The extensive cyberspace capabilities and coordination authorities that reside with USCYBERCOM make it well suited to lead many federal operations against unconventional cyberspace threats that can be expected to be external in nature. Internal responses will likely preclude the DOD from establishing itself as the lead authority, since its operations will, in most circumstances, be governed by stipulations of the PCA—and other relevant legislation. The DHS is likely the most logical organization to lead internal

[473] *See* generally EXAMPLES OF INTER-TITLE COOPERATION. *Supra* at Ch 3 s. (A)(2).

operations. It has an extensive capability for responding to domestic threats that is complimented by a leading role in coordinating cyberspace responses. There are intelligence operations that might be better served if led by one of the many agencies operating under Title 50, and the FBI is easily complemented by Title 10 authorities in their requirements to prosecute international criminals who commit crimes pursuant to 18 USC.

Table 3. Title Authority and Its Relation to Lead and Support Roles

Title Authority	Authority Role (check all that apply)	
	Lead	Support
6 USC		
10/32 USC		
14 USC		
18/28 USC		
50 USC		
SAD		

Under this format, planners can determine overall lead and support roles, and assign lead and support roles to each stage or aspect of operations.

Table 3 represents the minimum authority considerations needed to make inter-title determinations in support of cooperative cyberspace operations. The entries in this table are initially blank and must be filled in by the planners, which can be done in a variety of ways. As with Table 2, simpler operations will likely support spaces being used to specify leading and supporting organizations, units, or sub-units. For operations that are large, complicated, or contain multiple stages, these boxes will likely refer to documents that outline all assigned forces and their specific employment. Under this format, planners can determine overall lead and support roles, and also assign lead and support roles for each stage or aspect of an operation.

Table 3 is primarily intended to clarify the overall leading and supporting roles over the course of the operation, however, it is important to recognize that participation can be a very dynamic aspect of operations—especially those that are longer in duration. Simply put, leading and supporting roles can change throughout the course of an operation. This table allows for this dynamic change by allowing organizations operating under a given title authority to annotate forces that will be in leading and supporting roles. In the case of domestic support to homeland security, for example, Title 32 operators may initially be in a support role under SAD authorities. As the operation progresses, there may be a need to shift the role of lead authority to Title 10. This shift can be in response to some event or a planned aspect of the operation. None of these shifts in authority precludes continuity of operations. Instead, they inform operators, fiscal appropriations, and oversight bodies as to the source of authority from which all subsequent orders will be issued.

All of these shifts can be basically accounted for in the previous matrix, though for more complex operations, it is recommended that blocks simply refer to organizational units or sub-units with details annotated in attachments or references. The dynamics of these leading and supporting roles are critical at each stage of the operation and may be revisited or restructured as needed. This assists the operational planning process since it is altogether possible that agencies that are authorized to assist in the earlier stages of an operation might be statutorily precluded from assisting in the latter stages—and vice versa.[474]

Before moving on to the final framework, it is worthwhile to briefly draw attention to the numerous legal systems in which inter-title teams will operate. When planning for inter-title operations, it is important to understand the legal implications for any violations that may occur. It is likely a concern for these disparate court systems that form the basis for many of the fallacies that demand

[474] For more examples of lead and supporting authorities or dual-lead authorities, *see* generally APPENDIX C – Notable Examples of Lead and Supporting Authorities as They Pertain to Inter-Title Operations.

a prohibition against inter-title operations. Depending on the nature of the activity, or the sovereignty it affects, inter-title teams may be considered liable under one or more jurisdictions—depending on the nature and extent of a violation. The four most relevant court systems are shown in Table 4.

Table 4. International and Domestic Court Systems

Court Body	Governing Statutes
International Criminal Court (ICC)	Rome Statute[475]
Military Tribunal	Uniform Code of Military Justice (UCMJ)
Federal Court System	Federal Law
State Court System	State Law

This table lists potential legal systems and governing statutes that may be applicable when conducting inter-title operations.

In addition to these legal systems, governing authorities from foreign nations may be authorized by their own domestic legal systems to bring charges against all or some of the participants involved in inter-title cyberspace operations. Though not of immediate concern, complex extradition laws make this worthy of some consideration. The salient point here is that the level of liability to which inter-title operators are subject, may be different for each operation and it is an important consideration for each stage of action and to the operation as a whole.

D. INTER-TITLE COOPERATION MATRIX

In combining the isolated matrices from previous sections, the concluding framework incorporates demands for congressional oversight, considerations for fiscal appropriations, and the clear delineation of responsibilities and assignment of a lead authority. In its most basic sense, this framework is intended to leverage the unique capabilities of each organization in order to achieve national

[475] Although the United States as not formally recognized the Rome Statute, the ICC is not prevented from bringing charges against the United States or its citizens.

security objectives that may exist beyond the capability of any one single organization to achieve on its own. The final framework (Table 5), while likely adequate for planning and executing inter-title cyberspace operations, is still subject to a number of underlying assumptions and presuppositions.

One of these assumptions is that the operation is both legal and sanctioned by operational authorities. Far from being a prescription to enable organizations to advance their own objectives, the framework is built on cooperative agreements that have been entered into by authorities that are both competent and complicit—except were statutory authority authorizes forcible cooperation. Additionally, a major presupposition for this framework is that these operations are aligned to national security objectives. In the area of covert action, particularly, there is an emphatic prohibition against taking any action that is "intended to influence United States political processes, public opinion, policies, or media." This may be a presumption for most, but the end state objectives of every operation must be cognizant of the potential for collateral effects at each stage of the operation. Another key presumption is linked to the relevant and diverse legal systems to which inter-title operations can be simultaneously subject. In light of previous violations—like those that characterized inter-title operations during the L.A. Riots—it is presumed that appropriate training has been conducted to the extent necessary based on the nature and extent of each agency's participation. These training requirements should also reasonably account for potential contingency operations.

An item that remains unsettled from the previous section is the process by which congressional oversight can be sufficiently satisfied. Intelligence oversight committees generally believe that the conduct of intelligence activities—especially those involving covert action—carry great risks in the diplomatic arena and for national security. As such, a strong case might be made for advancing the intelligence committees as the final oversight reviewer. This, however, disregards concerns in fiscal reporting. It is more likely that the lead authority will be required to consolidate reporting and submit combined appropriations

requests through their relevant congressional committee—unlikely to be the intelligence oversight committees unless operations are primarily dependent on statutory authorizations from 50 USC. Aside from this argument, defaulting to the committee with the greatest potential for liability additionally fails to grasp that supporting title authorities fulfill a complementary role, no matter how important they are for operational success. Title 50 intelligence support to military operations is just one example of this. While Title 50 support may be critical to mission success, military forces may still choose to proceed with an operation even if they must proceed without the support of the intelligence committees.

Stepping back from the desires of the oversight committees, it becomes clear that the consternation is, in large part, due to the fact that Congress insists on aligning their committees to broad areas of activity instead of to the title authorities themselves.[476] To understand which committee has a more viable claim to final review, planners would be forced to take up the untenable position of attempting to apply every action to every possible statute—some actions being applicable to numerous statutes. Making this even more difficult is that the process is almost entirely incompatible with the format by which operations are planned. Instead, it is recommended that the statutory activities be vetted through their respective congressional committees and that final review be provided by the congressional oversight body that most closely aligns with the lead title authority in the operation. In the case of a Title 10 lead authority, the House and Senate Armed Services Committees would provide final review. In the case of a Title 50 lead authority, it would likely be the intelligence committees. In the case of a DHS-led operation, it may be more difficult to determine the committee with final review authority, but it would be significantly less complicated than the other alternative. As with many of the preceding arguments, this is one that primarily concerns policy. It is just as likely that the House and Senate will pass rules or legislation to adjust the way in which this process proceeds—irrespective of any recommendations outlined here.

[476] Wall, 141.

Table 5. Framework for Inter-Title Cyberspace Operations

Title Authority	**Oversight Body**	**Fiscal Responsibility** (check all that apply)			**Authority Role** (check all that apply)	
		Funds	Personnel	Reimbursement	Lead	Support
6 USC	HSGAC/CHS *(CS&T/T&I)*					
10/32 USC	SASC/HASC*					
14 USC	CS&T/T&I (HSGAC/CHS)					
18/28 USC	SJC/HJC					
50 USC	SSCI/HPSCI †					
SAD	State Committee					

* Under executive control of the Commander in Chief, activities pursuant to relevant authorities are, in general, only limited by the president.

† Current structures for congressional oversight make congressional approval, in general, a necessity for authorizing intelligence activities—to include covert activity. Note: Instructions for correctly filling out the framework are contained in preceding sections (Ch. 4 ss. (A),(B),(C)) with examples in the succeeding chapter (Ch. 5 ss. (A),(B)).

V. INTER-TITLE CYBERSPACE SCENARIOS

With the matrix complete, this chapter demonstrates utilization of the matrix to enable inter-title cyberspace operations. As such, it is important to complement the framework proposal with a prominent feature of cyberspace operations, which is the fact that they generally tend to encompass limited aspects of larger operations. Operations often center around non-cyberspace actors who, for one reason or another, require a cyberspace capability in order to achieve their objectives. While there are certainly operations that have significantly higher degrees of cyberspace purity, an increasing number of operations either provide support to or are themselves supported by kinetic operations that originate in the physical domains. The following scenarios represent these two worlds. The first scenario is a counterproliferation scenario that makes use of both traditional and cyber-forces, while the second scenario is more purely cyber as it depicts an attack against Southern California's electrical grid.

A. SCENARIO 1: INTER-TITLE CYBERSPACE SUPPORT TO COUNTERPROLIFERATION OPERATIONS

Scenario Setup

Introduction:	A Maltesian-flagged merchant ship, Motor Vessel (M/V) NANA ONE is alleged by an intelligence source to be transporting a known shipment of drugs and several suspicious canisters with unknown contents to a distribution facility in San Francisco, CA.
18 USC:	The vessel has been coordinating their shipments via email through an illicit criminal network with possible ties to terrorist groups based in the Indo-Pacific region. Intelligence sources have regular access to these correspondences and the FBI is seeking prosecution against some crewmembers of M/V NANA ONE under violations of 21 USC § 846 and 18 USC §§ 1030,1956.

14 USC: The FBI and U.S. Coast guard have agreed to joint leadership responsibilities with the Coast Guard using its coastal forces and cyber cadre to lead the operation while M/V NANA ONE is underway followed by the FBI assuming the role of lead authority for all operations subsequent to the vessel mooring pier-side at the distribution facility.

10 USC: The USCG does not have any medium or high-endurance cutters available to support this mission, and have requested the U.S. Navy to provide real time tracking and have transferred key personnel to the Navy warship in the event that a boarding of the vessel becomes necessary. All support requirements involve tracking and reporting between Honolulu, HI and San Francisco, CA.

50 USC: Intelligence assets from the NSA are providing SIGINT support to all involved entities and clandestine cyberspace operators have been authorized to intercept and report on any communications that are outbound or inbound to the vessel.

Relevant Information for the Inter-Title Framework

Authorities: 10 USC / 14 USC / 18 USC / 50 USC

Oversight:	10 USC:	SASC / HASC
	14 USC:	CS&T / T&I
	18 USC:	SJC / HJC
	50 USC:	SSCI / HPSCI
Fiscal Concerns:	10 USC:	Personnel / Reimbursement
	14 USC:	Funds / Personnel
	18 USC:	Funds / Personnel
	50 USC:	Personnel
Authority Role:	10 USC:	Support
	14 USC:	Lead
	18 USC:	Lead/Support
	50 USC:	Support

Table 6. Scenario 1: Completed Framework for Inter-Title Cyberspace Support to Counterproliferation Operations*

Title Authority	**Oversight Body**	**Fiscal Responsibility** (check/fill in all that apply)			**Authority Role** (check all that apply)	
		Funds	Personnel	Reimburs.	Lead	Support
10 USC	SASC/HASC	None[1]	~300 active duty	Waived[2]	N/A	DDG-102
14 USC	CS&T/T&I (HSGAC /CHS)	Yes (50%)[3]	42 Active Duty 7 Reservist 9 Auxiliary	No	D11 Command Center	- MSST SF - PACAREA TACLET (embarked DDG-102) - **CG PACCYBER**
18 USC	SJC/HJC	Yes (50%)[4]	20 Agents, 13 Support staff - 4 Linguists - 4 Intel Analysts - 5 Technicians	No	**Organized Crime Task Force (OCTF) Joint Operations Center (JOC)**	**OCTF JOC** (when necessary)
50 USC	SSCI/HPSCI	None[5]	**Yes**[5]	No	N/A	**Tactical Coordination Center (TCC)**[5]

[1] Expended funds will derive from appropriated funds (funding line PAC-H-A17). Any incidentals will be funded by lead authorities: 14 USC (Funding line D11-PAC-PD3) and 18 USC (Funding line OCTF-1-3).
[2] Pursuant to 10 USC § 377 (REF A – DOD REQUEST FOR WAIVER APPROVAL LETTER).
[3] Expended funds will derive from appropriated funds (funding line D11-PAC-PD1). Fair share of incidentals and funding for embarked PACAREA TACLET will be provided for from funding line D11-PAC-PD3.
[4] Expended funds will derive from appropriated funds (funding line OCND-4-2). Fair share of incidentals will be provided for from funding line OCTF-1-3.
[5] Details contained in classified attachments (ATTACHMENT 1)
* *DISCLAIMER*: All funding lines, references, attachments, and units in **bold font** are fictional. Any resemblance they may bear to actual organizational constructs is entirely coincidental.

Scenario Development

Inter-Title: *(10 USC)* The U.S. Navy ship is tracking M/V NANA ONE with a shipboard radar within territorial waters and intends to provide continued surveillance of the vessel until it is moored at the distribution facility.[478]

(14 USC) Coast Guard coastal patrol boats provide additional surveillance of the vessel as it enters the San Francisco Bay, but their presence paired with the U.S. Naval warship prompts the master of M/V NANA ONE to report the increased activity to their criminal contact.

(50 USC) Intelligence operators report the outgoing transmission to the USCG and FBI.

(*14 USC and 18 USC*) After brief discussions, the USCG decides to block any further email correspondence to or from the vessel as it pertains to the drug shipment. An email regarding port services is forwarded on to the ship, but an email from the criminal contact is intercepted and delivery is barred.

(*10 USC and 50 USC*) The position of M/V NANA ONE is continually updated by the U.S. Navy ship and validated by SIGINT reporting collected through provisions of FISA.

(*10 USC, 14 USC, 18 USC, and 50 USC*) As the ships moors, the master of M/V NANA ONE dispatches another email to an address that has yet to be observed over the course of this investigation. As the USCG turns over lead authority to the FBI, the email addressed is checked against a state criminal repository. To investigate further, the FBI directs the USCG coastal forces to stand-down until notified otherwise. Meanwhile, local law enforcement databases return a match for a suspected drug trafficker operating out of Southern California. The FBI then directs USCG cyber operators to forward the message to the intended recipient. Within a few hours, the suspected drug trafficker and the master of the vessel are arrested by USCG forces and FBI agents during the exchange. Over 800lbs of marijuana are seized from the hold of the ship, and the suspicious containers were found to be holding liquid cocaine totaling more than 1200kg.

[478] Pursuant to 10 USC § 374(b)(2)

B. SCENARIO 2: INTER-TITLE CYBERSPACE SUPPORT TO DEFENSE OF CRITICAL INFRASTRUCTURE

Scenario Setup

Introduction:	Pacific Gas and Electric Company (PG&E) is experiencing suspicious and potentially detrimental activity at numerous power plants in the portion of their electrical grid that ties in with Mexico's grid near the U.S.-Mexican border.
50 USC:	Intelligence analysts receive indications of a potential cyber attack along California's border with Mexico and generate an alert report through intelligence sharing channels.
6 USC:	Indications of potential cyber attacks are received by the NCCIC and immediately forwarded through the HSIN-CI from which alerts are disseminated to PG&E Corporate Headquarters, the California State Governor's Office, USCYBERCOM, US-CERT, ICS-CERT, and the Cyber National Guard Units responsible for supporting the California.
32 USC:	Cyber National Guard Units receive the alert and prepare to support operations.
10 USC:	USCYBERCOM National Mission Teams are in heightened alert and prepared to support operations.
SAD:	The state governor's office receives the alert and following deliberations with the regional director for PG&E network management, NCCIC, USCYBERCOM and the Cyber National Guard Unit, officially authorizes State Active Duty to respond to what is almost certainly a cyber attack against California's power grid. The responding organizations agree to a phased operational approach that has the potential to shift lead authority to any title authority except 50 USC.

Relevant Information for the Inter-Title Framework

Authorities: 6 USC / 10 USC / 32 USC / 50 USC / SAD

Oversight:

6 USC:	HSGAC / CHS
10 USC:	SASC / HASC
32 USC:	SASC / HASC
50 USC:	SSCI / HPSCI
SAD:	State Governor

Fiscal Concerns:	6 USC:	Funds / Personnel
	10 USC:	Funds / Personnel / Reimbursement
	32 USC:	Funds / Personnel
	50 USC:	Personnel
	SAD:	Funds
Authority Role:	6 USC:	Lead / Support
	10 USC:	Lead / Support
	32 USC:	Lead / Support
	50 USC:	Support
	SAD:	Lead

Table 7. Scenario 2: Completed Framework for Inter-Title Cyberspace Support to Defense of Critical Infrastructure

Title Authority	**Oversight Body**	**Fiscal Responsibility** (check all that apply)			**Authority Role** (check all that apply)	
		Funds	Personnel	Reimbursement	Lead	Support
6 USC	HSGAC/CHS	Yes (100%)[1]	Yes[2]	No	X[3]	X[4]
10 USC	SASC/HASC	Yes (100%)[1]	Yes[2]	Yes[5]	X[3]	X[4]
32 USC	SASC/HASC	Yes (100%)[1]	Yes[2]	No	X[3]	X[4]
50 USC	SSCI/HPSCI	None[6]	Yes[6]	No		X[6]
SAD	Governor	Yes (100%)[1]	No	No	X[3]	

[1] Details contained in ATTACHMENT 2 – FISCAL ASSESSMENT PLAN (in accordance with ATTACHMENT 1)
[2] Details contained in ATTACHMENT 3 – PERSONNEL SUPPORT & ASSIGNMENT PLAN (in accordance with ATTACHMENT 1)
[3] Details contained in ATTACHMENT 4 – LEAD ROLES AND AUTHORITIES (in accordance with ATTACHMENT 1)
[4] Details contained in ATTACHMENT 7 – SUPPORT ROLES
[5] Pursuant to 10 USC § 377 (in accordance with ATTACHMENT 2)
[6] Details contained in classified attachments (ATTACHMENTS 8 and 9)

Scenario Development

Inter-Title: *(SAD, 6 USC, 10 USC, 32 USC, and 50 USC)* The state governor's office is directing the Cyber National Guard efforts and coordinating backup restoration efforts with PG&E. Intelligence reporting indicates that the threat source may be originating from a remote location outside of California's power grid, but analysis is inconclusive. The governor desires to direct restoration efforts, but now requires federal assistance as it is now clear that the scope and costs are more extensive than had originally been anticipated. The NCCIC has been coordinating all efforts thus far and has updated all parties to the governor's request and the president's subsequent approval to federalize the cyber-forces and allow the USCYBERCOM to provide assistance.

(*6 USC, 10 USC, 32 USC, and 50 USC*) The electrical grid continues to degrade and the DHS and USCYBERCOM have realized that the National Guard forces do not have the requisite training to use the advanced cyber capabilities necessary to isolate and neutralize the attacks. After significant deliberations between DHS, USCYBERCOM, and the president, an executive order is issued—against the governor's wishes—to fully federalize the operation by way of a declaration of an emergency.

(*6 USC, 10 USC, 50 USC*) Instead of placing USCYBERCOM as the lead title authority, all parties agree that it would be in the best interest of the operation if DHS took over domestic operations to stabilize the power grid. US-CERT and ICS-CERT immediately set to work to diagnose the source and nature of the attacks. As efforts get underway, intelligence reporting reveals two key pieces of information. The first is that the attacks were originating in the Indo-Pacific region. The second is that the attacks were being directed against Mexico's power grid, which was affecting power along the border where the U.S. and Mexico share infrastructure.

(*6 USC, 10 USC, 50 USC*) In light of these new developments, lead authority is shifted to USCYBERCOM. The State Department is able to negotiate authorization from the Mexican administration for USCYBERCOM to operate in and through a limited number of Mexican networks and infrastructure in order to bring quick resolution to the problem. Using intelligence to support cyber fires, NMT operators make use of the extensive cyber-munitions to provide Defensive Cyber Operations, Response Actions (DCO-RA) actions against the cyber perpetrators and to restore the electrical grid to full operation.

VI. CONCLUSIONS AND RECOMMENDATIONS FOR FUTURE RESEARCH

A. CONCLUSIONS AND SUMMARY

There were many challenges associated with creating the preceding framework to support inter-title cyberspace operations. Much of the commentary of the first three chapters lays out the context for cyberspace operations and then commits a great deal of space to clarifying, revealing, and debunking much of the information and misinformation associated with inter-title operations. The material is arguably dense and much of the thoroughness is intended to corral objections that are only tangentially opposed to inter-title operations. With many of these objections having been addressed in Chapters I–III, Chapter IV is focused on the simpler task of building the framework that cyberspace operational planners can leverage to enable inter-title cooperation. Having set aside myth and misinformation, the framework recognizes that there are three major hurdles that planners must address in order to establish inter-title operations that are legally compliant. These three concerns have been identified as congressional oversight and compliance, fiscal requirements, and the assignment of responsibilities and command authority. These three areas are often held captive by a variety of congressional and executive policies, but they are nonetheless, viable avenues from the perspective of the United States Code. This is not to say that policy is irrelevant but simply an effort to understand the extent to which inter-title operations are permissible by federal law. As such, the following four points summarize crucial conclusions wrought from the previous five chapters.

1. Understand the Limitations of Policy

There are certainly consequences—even legal repercussions—for failing to follow policy and procedure. Because of this, planners are often hampered, not by legislation, but by policies masquerading as law. Understanding the difference between the two is crucial for planning and executing inter-title operations. This is

not to say that policy is unnecessary or an unwelcome guest in inter-title discussions. When compared with the legislative process, policy tends to have the advantage of being more flexible, and its potential for change is typically subject to shorter timelines. However, in the development of an operation, planners are likely to avoid courses of action that appear to conflict with a standing policy, even if the context for that policy is not understood. Worse yet, the absence of a clearly defined policy may dissuade approval authorities from pursuing a specific course even if its suggested actions are statutorily authorized.

It is therefore of utmost importance to understand the limitations of policy and the legislative authorities from which they stem. This balanced approach will, on the one hand, enable planners to perceive situations were standing policies are irrelevant and seek out relevant legislation to reinforce operational plans. On the other hand, if overly restrictive policies are playing a substantial role in operations, an understanding of their derivative legislation can be used to justify temporary memoranda or waivers that will allow operations to proceed unimpeded. In order to be effective, however, operational planners need to be familiar with both policy and legislation.

2. Comply with Congressional Oversight

The overabundance of legislation at both the domestic and international level are often exacerbated by competing political agendas and power struggles between the governing branches of the U.S. government. The results vary, but it is not uncommon for the Executive Branch to be met by frequent and fierce congressional opposition when it attempts to wield power or overextend its authority. Congressional oversight committees are partly the result of this dynamic and partly responsible sustaining it. In the ongoing debates over jurisdiction amongst title authorities, the congressional call for compliance must be met. Marrying up the jurisdictions of the congressional committees with the jurisdictions of the title authorities is a difficult but necessary task in enabling inter-title cyberspace operations. Difficulties arise due to the complex

organizational structure of the House and Senate committees, which is not directly aligned with title authorities, but they can also be the result of disinformation and jurisdictional misperceptions that are resident within the committee system itself—as is often the case with Title 10 intelligence and Title 50 intelligence activities. Despite the complexity, relevant congressional committees must be identified and operations must be reported or vetted by them as appropriate. The extent to which the congressional committee can approve, disapprove, or even defund an operation is dependent on a number of factors. It is therefore critical to first understand what is authorized through legislation and then to understand the extent to which each committee is able to validate or invalidate a given activity.

3. Ensure Fiscal Integrity

Previous discussions on fiscal requirements suggested that this step would likely be the most difficult. While the relative difficulties of satisfying each element of the framework will vary from operation to operation, ensuring fiscal integrity should generally be expected to be the most difficult. Ironically, the increasingly austere fiscal environment supplies much of the motivation for aggregating resources in order to remain both effective and relevant. Planners and staff members must not only understand the legislative authorities that are active in each operation, but also be capable of adequately linking them to a budget line item that has been approved by Congress. In cases where numerous funding lines are being pooled to support aspects of operations with jurisdictional overlap, planners must make “fair share” determinations. In addition to this, personnel must be allocated and reimbursement expenses must be identified. All of this must be done in accordance with title authorities and relevant legislation. As proposed in Chapter IV, many of these difficulties can be eased by establishing fiscal norms for inter-title operations through memoranda of agreement or a more robust policy that consolidates legislative requirements.

4. Establish a Competent Lead Authority

Ideally, this should be the easiest requirement to fulfill, but it is often subject to limitations that are not immediately apparent. Identifying the lead and supporting title authorities—being certain to account for legislated limitations like those found in the PCA—is the first basic step for determining a competent lead authority. After this, however, there is a need to identify whether lead title authorities have the experience necessary to lead these types of operations or whether they have staffs available to coordinate inter-title activities. In addition to this, determinations must be made as to the surge capacity and sustainability of the lead title authority. Many agencies, organizations, and departments do not have the experience or the personnel to coordinate large or long-term operations. These aspects must be factored in when determining the nature and extent of supporting and leading roles for inter-title operations.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

With the completion of the inter-title framework, there remains a great need for further research to further clarify the best means by which a path can be clear to enable these operations to be planned and executed along reasonably shorter timelines. The following recommendations are areas that will lead to less obstructions and greater efficiency in mission planning and execution.

1. Simplifying Congressional Oversight

For all the countless papers published and innumerable task forces assembled, the disruptive organizational structure of congressional oversight has seen little change. An acceptable process for simplifying congressional oversight is in need of significant research and relentless advocacy. It is nearly undisputed that cyberspace poses an immense challenge and harbors numerous threats to U.S. national security. Efforts to address these threats effectively are often mired in disputes over which organization and congressional committee have jurisdiction. Overlapping jurisdictions in cyberspace are almost certainly a

necessity, but the complexity of the issue has led to inconsistent responses from congressional oversight committees. A security executive, Arif Alikhan, observes:

> Cybersecurity is not an issue about partisanship because many of the proposed bills have had bipartisan support. It's really an issue of so many different committees that all have their particular interest and they can't get together with a coherent plan to pass a law to help protect the United States against very real cyberthreats.[479]

Contested jurisdictions of oversight, inconsistent methods of approval, and an inability to pass cyber legislation[480] are all indicative of a system of congressional oversight that is in need of clarity and reform.

2. In-Depth Fiscal Analysis for Supporting Inter-Title Operations

Federal appropriations remain a prime example of the byzantine processes that are stereotypically associated with the U.S. government. To begin with, appropriations have no consistent vehicle through which they must be passed and find themselves spread across a number of bills that can have little or no relevance to the appropriation itself. Secondly, the purpose for proposing appropriations legislation and the means by which it is passed are sometimes indiscernible. In some cases, fiscal appropriations can result from annual legislation, while in other cases, continuing resolutions can perpetually authorize appropriations with no requirement that it ever be included in regular legislation. Understanding fiscal appropriations also requires comprehension of all relevant title authorities, acts and amendments—for which there may be one or many relevant appropriations. To complicate matters further, Authorization Acts often are employed to modify funding to a specific agency or programs of record.[481] For any one of the innumerable paths through which appropriations can be

---

[479] DHS Congressional Oversight Task Force, 16.

[480] *See supra* at Ch. 2 s. (C)(4)(e). Under H.R. 3523, the Cybersecurity Act of 2015 (containing CISA), was surreptitiously passed as part of an omnibus bill. The main tenets of CISA, however, were originally proposed by the HPSCI as early as 2011.

[481] *See* RELATIONSHIP BETWEEN AUTHORIZATION AND APPROPRIATIONS MEASURES. CRS, *The Congressional Appropriations Process: An Introduction*, 10–12.

determined, there remains a need to align inter-title actions with the complex system of appropriations and to design understandable methods for inter-title disbursements.

3. Inter-Title Planning Models

Most planning models that acknowledge the need for inter-title cooperation, start from the perspective of a single organization and, as needs are recognized, external organizations are folded in through an elaborate network of command centers and agency liaisons. It follows an approach to planning that prioritizes an “inside-out” methodology and benefits from having most subject matter experts as resident within the organization. This approach is prevalent and has accompanied operational success for decades that have been characterized by clearly defined lanes and little interaction outside of one’s own agency or organization. The message from the 9/11 Commission, however, is that organizational isolation is more of a liability than an asset. It is therefore surprising that few planning models—possibly none—start with a broad inter-title framework and narrow the focus as roles and responsibilities of participating agencies are more clearly defined.

Though inconclusive, cyberspace operations appear poised to benefit from an “outside-in” approach that assumes the participation of many authorities and discards or reduces inter-title roles as the planning process more clearly defines the boundaries of the operation. The DOD uses the Joint Operational Planning Process (JOPP) and the FBI uses the Domestic Investigations and Operations Guide (DIOG). Each agency has an equivalent planning guide, which assists agencies in consolidating allies and assets to aid in accomplishing organizational goals. Cyberspace operations, however, would likely benefit from a detailed inter-title planning process that is designed by a commission of planners throughout various organizations and operating under every major title authority.

C. A FINAL WORD

Having completed this work, it is difficult to imagine that its conclusions will be fully accepted without protest or that it will be immediately incorporated into the planning process. Changing policy and attitudes toward federal action in cyberspace is made especially difficult given that most U.S. citizens—most executive and congressional employees for that matter—do not feel that they have enough information to make an informed decision about the matter. The fact of the matter is that cyberspace operations continue to be entrusted to a federal minority whose tactics, techniques, policies, and permissions are enumerated with a great deal of secrecy.

The conclusions presented in this thesis do not portend an answer for these dilemmas, but instead, offer a legal solution for many of the supposed barriers to advancing U.S. national security interests in cyberspace. The stakes in cyberspace are high and the challenges to inter-title operations are many. The technological gap is likely closing between the United States and adversary nations. More than that, criminal organizations and even political activists are increasingly posing a threat to U.S. national security. With a myriad of threats converging upon numerous sectors of the United States, it is unlikely that federal agencies and organizations will be capable of providing resolution while operating under limited cooperation or in isolation from one another.

While speaking at an Air Force Association (AFA) conference, retired Air Force General Chuck Horner said of cyberspace operations, "I learned this: Don't ever ask permission. Just do it, and apologize afterwards."[482] This disturbing "just-do-it" mentality is something that operational planners can avoid by using the presented framework. Cyber planners and mission commanders have broad and sufficient statutory authorities under the allowances of the United States Code—among other federal legislation at large—to conduct inter-title operations

[482] Jennifer Hlad, "Just Do It," *Air Force Magazine*, March 10, 2016, http://www.airforcemag.com/DRArchive/Pages/2016/March%202016/March%2010%202016/Just-Do-It.aspx.

without having to “ask permission” and without constructing a post-mission apology. Planners and commanders must educate themselves and develop plans that clearly communicate the role of each organization and the statutory authorities under which they will operate. In this way, inter-title cyberspace operations can be rescued from intimidation and grounded confidently within the framework of the law.

APPENDIX A. NOTABLE VIOLATIONS AND EXCEPTIONS TO THE POSSE COMITATUS ACT

Conduct	Explanation	Regulation	Statute	Case	Relationship to PCA
Regulate, Proscribe, or Compel Test: Did the military regulate, proscribe, or compel civilians as part of the operation?	This test is met if the military exerts any type of direct control or coercive power over civilians, such as road blocks, searches, or detentions	DoD 5525.5	10 USC § 375	US v. McArthur1	Violation
Direct Active Use Test: Did the military directly and actively participate in the law enforcement activity?	Transportation, furnishing equipment, supplies, or services, i.e.…providing medical care to prisoners is "indirect use" and therefore permitted. If, however, the military takes a direct role, such as operating equipment or providing direct assistance, the action is unless covered by an exception.	DoD 5525.5	10 USC § 372-375	US v. Red Feather US v Hartley	Violation
Pervasiveness Test: Did the military activity pervade the activities of the civilian authorities?	Combined operations with law enforcement meet this test, even if the only participation is decision making during the execution of the operation. The PCA does not prohibit "Advice", by itself, unless it is "controlling" to the point of pervading the activities of civilian authorities.	DoD 5525.5		US v. Jaramillo	Violation
Extraterritorial conduct of a military force	When military authorities enforce US law outside the US, whether or not the suspect is a US Citizen, or when they assist foreign officials enforce their own laws. Arrest of foreign nationals overseas.	DoD 5525.5 (requires SecDef approval)	See US v. KhaN, (holding that 10 USC § 372 applies extraterritorially)	Chandler v. US1	Exception
Indirect Involvement	Incidental or conduct supporting law enforcement activities, such as providing equipment, training, maintenance, and nonbinding advice.	DoD 5525.5	10 USC § 372-377	US v. Yunis	Exception
Military Law Enforcement on military installations	Law Enforcement conduct directed against service members and civilians on military installations.	DoD 5525.5	18 USC § 1382	US v. Banks	Exception
Commanders' Inherent authority to Repel attacks, or protect immediate loss of life	When commanders exercise their inherent authority to protect their installation from attack or take immediate steps to protect the loss of life.	DoD 5525.5 DoD 3025.12	10 USC § 809(e)	Cafeteria Workers v. McElroy	Exception

Adapted from: APPENDIX 1 and 2. Donald J. Currier, "The Posse Comitatus Act: A Harmless Relic from the Post-Reconstruction ERA or a Legal Impediment to Transformation," research project in U.S. Army War College (Carlisle, PA: USAWC, 2003), 25–28, http://handle.dtic.mil/100.2/ADA413494.

Conduct	Explanation	Regulation	Statute	Case	Relationship to PCA
National Guard	The National Guard, when used in a "state status."	DoD 5525.5		Gilbert v. US	Exception
Military Purpose Doctrine	The PCA does not apply to actions performed primarily for a military purpose, such as Investigating crimes against the military.	DoD 5525.5		Cafeteria Workers v. McElroy	Exception
Riot, Insurrection or lawlessness	Extraordinary cases where the President employs his Constitutional authority to maintain order.	DoD 5525.5 DoD 3025.12		10 USC §§ 331-334 10 USC § 12406 US Const., Art II	Exception
Dignitary Protection	Protection of members of Congress, executive Cabinet members, Supreme Court Justices, diplomats, President, VP & Whitehouse staff.	DoD 5525.5	18 USC §§ 112, 116, 351(g), 1201(f), 1751		Exception
Disaster Relief	Troops providing relief during times of National Disaster.	DoD 5525.5 DoD 3025.1 DoD 3025.15	Stafford Act (42 USC §§ 5121, *et seq.*)		Exception
Quarantine	If an individual has a specifically identified communicable disease, Heath Authorities may detain them. The President may use the military to assist the Surgeon General execute his duties.	DoD 5525.5 DoD 6000.12	42 USC §§ 97, 264 (d)		Exception
Drug Interdiction	Sharing of information and Intelligence.	DoD 5525.5	10 USC § 371		Exception
Customs & Immigration	Sharing of information and Intelligence.	DoD 5525.5	50 USC § 220		Exception
Customs & Immigration	Sharing of equipment and facilities.	DoD 5525.5	10 USC § 372		Exception
WMD/E & Protection of Nuclear Materials	Provide Assistance to Dept. of Justice where a biological or chemical weapon of mass destruction poses a serious threat and civilian authorities require DoD	DoD 5525.5	10 USC §§ 382, 831 50 USC §§ 2(1), 2301 18 USC § 831		Exception
Protecting US Forests & Fisheries	Removing enclosures from public lands.	DoD 5525.5	42 USC § 1065 16 USC §§ 23, 593, 1861(a)		Exception
Indirect cooperation	Loan of Equipment to other agencies.		31 USC § 1535	US V. Jarmillo	Exception

Adapted from: APPENDIX 2. Currier, 27–28.

APPENDIX B. QUICK REFERENCE GUIDE FOR THE STORED COMMUNICATIONS ACT

	Voluntary Disclosure Allowed?		How to Compel Disclosure	
	Public Provider	**Non-Public**	**Public Provider**	**Non-Public**
Basic subscriber, session, and billing information•	No, unless §2702(c) exception applies *§ 2702(a)(3)*	Yes *§ 2702(a)(3)*	Subpoena; 2703(d) order; or search warrant *§ 2703(c)(2)*	Subpoena; 2703(d) order; or search warrant *§ 2703(c)(2)*
Other transactional and account records	No, unless §2702(c) exception applies *§ 2702(a)(3)*	Yes *§ 2702(a)(3)*	2703(d) order or search warrant *§ 2703(c)(1)*	2703(d) order or search warrant *§ 2703(c)(1)*
Retrieved communications and the content of other stored files#	No, unless § 2702(b) exception applies *§ 2702(a)(2)*	Yes *§ 2702(a)(2)*	Subpoena with notice; 2703(d) order with notice; or search warrant* *§ 2703(b)*	Subpoena; SCA does not apply* *§ 2711(2)*
Unretrieved communications, including email and voice mail (in electronic storage more than 180 days)†	No, unless § 2702(b) exception applies *§ 2702(a)(1)*	Yes *§ 2702(a)(1)*	Subpoena with notice; 2703(d) order with notice; or search warrant *§ 2703(a), (b)*	Subpoena with notice; 2703(d) order with notice; or search warrant *§ 2703(a), (b)*
Unretrieved communications, including email and voice mail (in electronic storage 180 days or less)†	No, unless § 2702(b) exception applies *§ 2702(a)(1)*	Yes *§ 2702(a)(1)*	Search warrant *§ 2703(a)*	Search warrant *§ 2703(a)*

• *See* 18 U.S.C. § 2703(c)(2) for listing of information covered. This information includes local and long distance telephone connection records and records of session times and durations as well as IP addresses assigned to the user during the Internet connections.

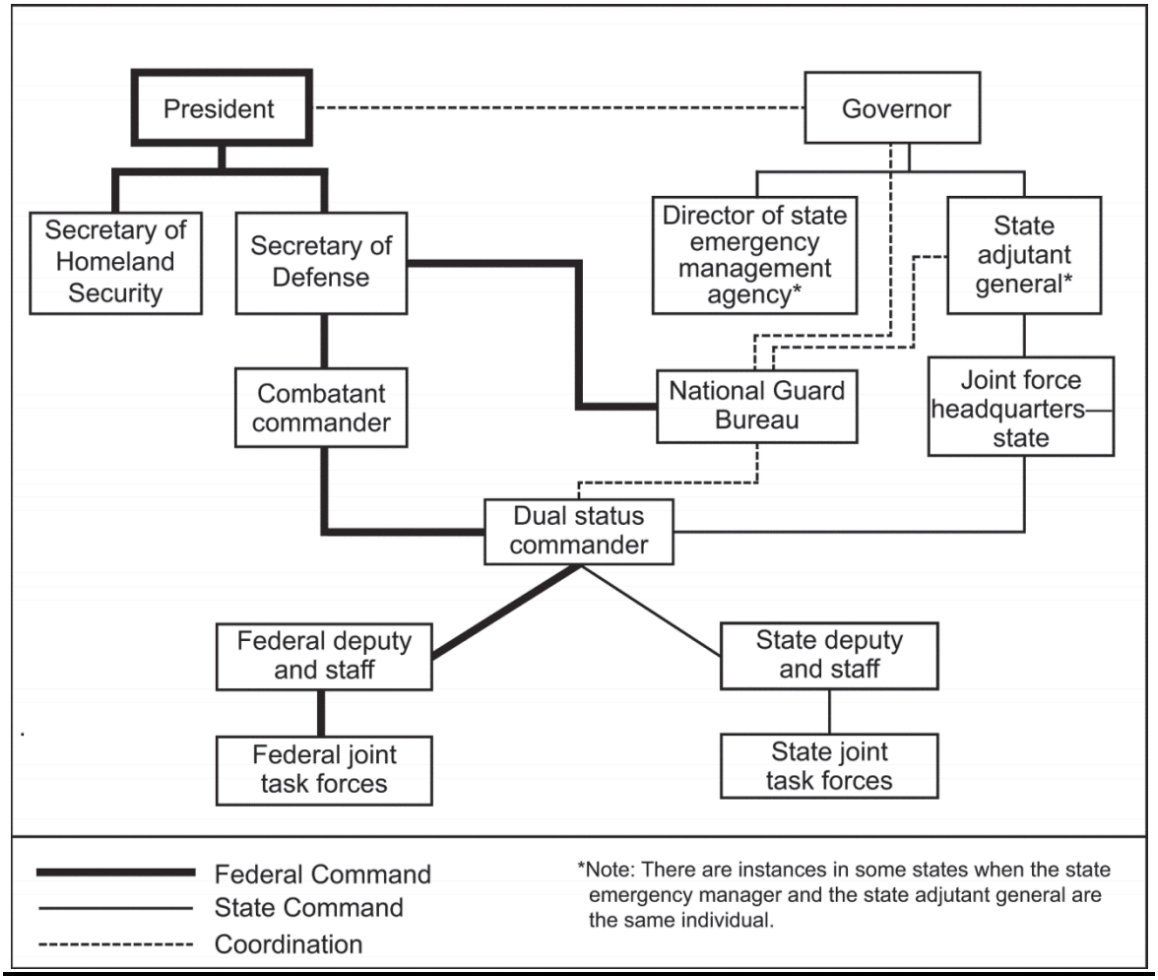
† Includes the content of voice communications.

* For investigations occurring in the Ninth Circuit, *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), requires use of a search warrant unless the communications have been in storage for more than 180 days. Some providers follow *Theofel* even outside the Ninth Circuit; contact CCIPS at (202) 514-1026 if you have an appropriate case to litigate this issue.

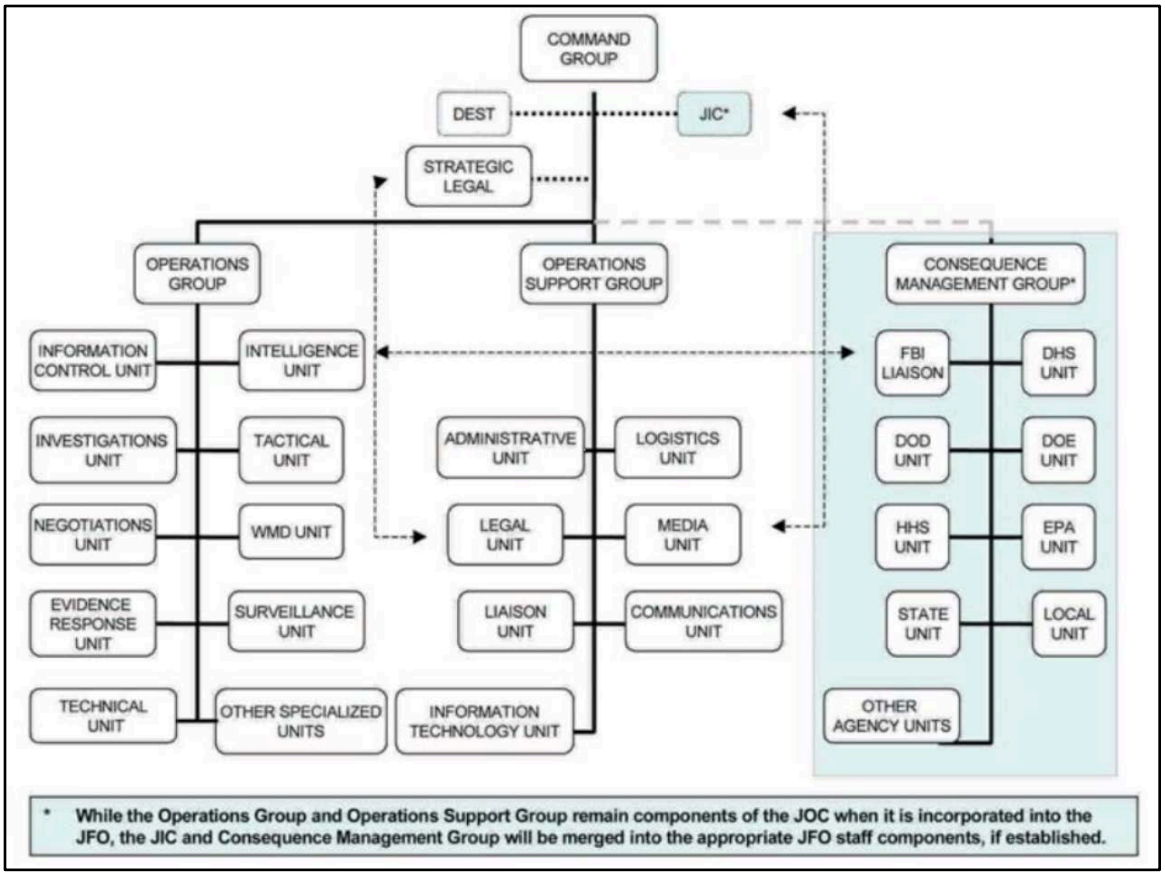
Source: CCIPS, "Searching and Seizing Computers and Obtaining Electronic Evidence In Criminal Investigations," 138. All references pursuant to 18 USC.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. NOTABLE EXAMPLES OF LEAD AND SUPPORTING AUTHORITIES AS THEY PERTAIN TO INTER-TITLE OPERATIONS



Source: ALSA, *Multi-Service Tactics, Techniques, And Procedures for Defense Support of Civil Authorities (DSCA)*, 11. The figure depicts the proposed structure for a dual status commander (DSC). It incorporates only SAD, Title 10 and Title 32 despite the fact that Title 18 and Title 14 are often involved in Defense Support of Civil Authorities.



Source: Center for Army Lessons Learned, *Catastrophic Disaster Response Staff Officer's Handbook*, No. 06-8 (Fort Leavenworth, KS: Combined Arms Center, 2006), 158, http://usacac.army.mil/sites/default/files/ publications/06-08.pdf. The figure depicts the Joint Operations Center (JOC), which is an "interagency command and control center for managing interagency preparation for, and the law enforcement and investigative response to, a credible terrorist threat or incident."

LIST OF REFERENCES

Adler, Adam J. “Dual Sovereignty, Due Process, and Duplicative Punishment: A New Solution to an Old Problem.” *The Yale Law Journal* 124, no. 2 (November 2014): 448–84. http://www.yalelawjournal.org/note/dual-sovereignty-due-process-and-duplicative-punishment-a-new-solution-to-an-old-problem.

Aftergood, Steven. “Reducing Overclassification through Accountability.” *Federation of American Scientists*, October 6, 2011. http://fas.org/blogs/secrecy/2011/10/brennan_ctr_report.

Agustina, Jose R. “Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect.” *International Journal of Cyber Criminology* 9, mo., (January–June, 2015): 35–54. doi: 10.5281/zenodo.22239.

Alderman, Ellan, and Caroline Kennedy. *The Right to Privacy*. New York: Alfred A Knopf, 1995.

Allen, Craig H. *Maritime Counterproliferation Operations and the Rule of Law*. Westport, CT: Praeger, 2007.

Anthony, Sebastian. “France Looking at Banning TOR and Public WiFi.” *ArsTechnica*, December 7, 2015. http://arstechnica.com/tech-policy/2015/12/france-looking-at-banning-tor-blocking-public-wi-fi.

Barrett, Mark, Dick Bedford, Elizabeth Skinner and Eva Vergles. *Assured Access to the Global Commons*. Norfolk, VA: NATO Headquarters, 2011. http://www.act.nato.int/images/stories/events/2010/gc/aagc_finalreport.pdf.

Basulto, Dominic. “We've Outgrown the Traditional Notions of Privacy.” *Washington Post*, February 12, 2015. http://www.realcleartechnology.com/2015/02/12/we039ve_outgrown_the_traditional_notions_of_privacy_25650.html.

Bazan, Elizabeth B. *P.L. 110–55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act* (CRS Report No. RL34143). Washington DC: Congressional Research Service, February 14, 2008. https://www.fas.org/ sgp/crs/intel/RL34143.pdf.

———. *The Foreign Intelligence Surveillance Act: Overview and Modifications*. New York: Nova Science, 2008.

Beckler, Mark M. “Insurrection Act Restored: States Likely to Maintain Authority Over National Guard During Domestic Emergencies.” Monograph, United States Army Command and General Staff College, 2008. http://www.dtic.mil/dtic/tr/fulltext/u2/a484794.pdf.

Bennett, Cory. “Cybesecurity’s Winners and Losers.” *The Hill*, December 19, 2015. http://thehill.com/policy/cybersecurity/263785-cybesecuritys-winners-and-losers.

Birkland, Thomas. *Lessons of Disaster: Policy Change after Catastrophic Events*. Washington DC: Georgetown University Press, 2006.

Bobbitt, Philip. *The Shield of Achilles: War, Peace, and the Course of History*. New York: Anchor Books, 2003.

Bowman, Steve, Lawrence Kapp, and Amy Belasco. *Hurricane Katrina: DOD Disaster Response* (CRS Report No. RL33095). Washington DC: Congressional Research Service, September 19, 2005. https://www.fas.org/sgp/crs/natsec/ RL33095.pdf.

Bowman-Grieve, Lorraine. “Cyberterrorism and Moral Panics: A Reflection On the Discourse of Cyberterrorism.” In *Terrorism Online: Politics, Law and Technology*, edited by Lee Jarvis, Stuart Macdonald, and Thomas M. Chen. New York: Routledge, 2015.

Boyle, Ashley S. *Fact Sheet: U.S.C. Title 10, Title 22, and Title 50, American Security Project*. Washington DC: American Security Project, 2012. http://www.americansecurityproject.org/ASP%20Reports/Ref%200073%20-%20U.S.C.%20Title%2010%2C%20Title%2022%2C%20and%20Title50.pdf.

Bradbury, Stephen G. “RE: Application of 18 U.S.C. §§ 2340–2340A to Certain Techniques That May Be Used in the Interrogation of a High Value al Qaeda Detainee.” Memorandum for John A. Rizzo, Senior Deputy General Counsel, Central Intelligence Agency, May 10, 2005. https://www.justice.gov/sites/default/files/olc/legacy/2013/10/21/memo-bradbury2005-3.pdf.

Brenner, Susan W. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 3rd edition. Edited by Eoghan Casey. New York: Academic Press, 2011.

Brown, Archie. *The Rise and Fall of Communism*. London: The Bodley Head, 2009.

Brown, Chris, Desmond Lee, Colin Scott, and Daniel Strunk. *American Cyber Insecurity: The Growing Danger of Cyber Attacks*. Durham, NC: Duke University, 2014. http://hdl.handle.net/10161/8881.

Burnett, John. “More Stories Emerge of Rapes in Post-Katrina Chaos.” *National Public Radio*, December 21, 2005. http://www.npr.org/templates/story/story.php?storyId=5063796.

Bush, George H.W. "Address to the Nation on the Civil Disturbances in Los Angeles, California.” May 1, 1992. Online by Gerhard Peters and John T. Woolley, *The American Presidency Project*. http://www.presidency.ucsb.edu/ws/?pid=20910.

Center, Mandiant Intelligence. "APT 1: Exposing One of China’s Cyber Espionage Units.” *Mandiant Corporation*, February 18, 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

———. "M-Trends 2016.” *Mandiant Corporation*, February, 2016. Available for download at https://www2.fireeye.com/M-Trends-2016.html.

Center for Strategic and International Studies. *Net Losses: Estimating the Global Cost of Cybercrime. Economic Impact of Cybercrime II*. Santa Clara, CA: McAfee, June 2014. http://www.mcafee.com/hk/resources/reports/rp-economic-impact-cybercrime2.pdf.

Center for Strategic and International Studies and Business Executives for National Security. *Untangling the Web: Congressional Oversight and the Department of Homeland Security*. Washington DC: CSIS and BENS, December 10, 2004. http://csis.org/files/attachments/041210_dhs_whitepaper.pdf.

Chesney, Robert M. “Beyond The Battlefield, Beyond Al Qaeda: The Destabilizing Legal Architecture of Counterterrorism.” *Michigan Law Review* 112, no. 2 (November 2013): 163–224. http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1036&context=mlr.

———. “Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate.” *Journal of National Security Law & Policy* 5 (2012): 539–629. doi: 10.2139/ssrn.1945392.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Harper Collins, 2010.

Cooke, Edward F. *A Detailed Analysis of the Constitution*, 7th edition. Lanham, MD: Rowman & Littlefield, 2002.

Cooper, Christopher, and Robert Block. *Hurricane Katrina and the Failure of Homeland Security*. New York: Henry Holt, 2006.

Cox, Ana Marie. "Who Should We Fear More with Our Data: The Government or Companies?" *Guardian*, January 20, 2014. http://www.theguardian.com/commentisfree/2014/jan/20/obama-nsa-reform-companies-spying-data.

Cramer, Clayton E. *For the Defense of Themselves and the State: The Original Intent and Judicial Interpretation of the Right to Keep and Bear Arms*. Westport, CT: Praeger, 1994.

Crockett, Danielle. "The Insurrection Act and Executive Power to Respond with Force to Natural Disasters." Paper prepared for Law 224.9: Disasters & the Law, University of California Berkeley School of Law, 2007. https://www.law.berkeley.edu/library/resources/disasters/Crockett.pdf.

Cunningham, Oliver. "The Humanitarian Aid Regime in the Republic of NGOs: The Fallacy of 'Building Back Better." *Josef Korbel Journal of Advanced International Studies* 4 (Summer 2012): 101–26.

Currier, Donald J. "The Posse Comitatus Act: A Harmless Relic from the Post-Reconstruction ERA or a Legal Impediment to Transformation." United States Army War College. Carlisle, PA: U.S. Army War College, 2003. http://handle.dtic.mil/100.2/ADA413494.

Danilovic, Vesna. *When Stakes Are High: Deterrence and Conflict Among Major Powers*. Ann Arbor, MI: University of Michigan Press, 2002.

Davis, Philip Adam. "The Defamation of Choice-of-Law in Cyberspace: Countering the View that the Restatement (Second) of Conflict of Laws is Inadequate to Navigate the Borderless Reaches of the Intangible Frontier." *Federal Communications Law Journal* 54, no. 2 (March 2002): 339–64. http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1299&context=fclj.

Delk, James. *Fires & Furies: The L.A. Riots, What Really Happened*. Palm Springs, CA: ETC, 1995.

Denning, Peter J. "Hastily Formed Networks." *Communications of the ACM* 49, no. 4 (April 2006): 15–20. http://denninginstitute.com/pjd/PUBS/CACMcols/cacmApr06.pdf.

Delaney, Donald P., Dorothy E. Denning, John Kaye and Alan R. McDonald. *Wiretap Laws and Procedures: What Happens When the U.S. Government Taps a Line*. White paper distributed by D.E. Denning, Professor and Chair Computer Science Department at Georgetown University. Washington DC: Georgetown University, September 23, 1993. http://faculty.nps.edu/dedennin/publications/WiretapLawsProcedures.txt.

Dempsey, John S., and Linda S. Forst. *An Introduction to Policing*, 5th edition. Clifton Park, NY: Delmar, 2009.

Ebbighausen, John H. "Unity of Command for Homeland Security: Title 32, Title 10, Or A Combination." Master's thesis, U.S. Army Command and General Staff College, June 16, 2006. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA451789.

Economist Intelligence Unit, "Democracy Index 2014," *Economist*. Accessed November 4, 2015 http://www.eiu.com/democracy2014.

Egan, Mark. "Rapes, Killings Hit Katrina Refugees in New Orleans." *Reuters*, September 4, 2005. Archived at http://www.redorbit.com/news/general/229546/rapeskillings_hit_katrina_refugees_in_new_orleans.

Elsea, Jennifer K. *Terrorism and the Law of War: Trying Terrorists as War Criminals before Military Commissions* (CRS Report No. RL31191). Washington DC: Congressional Research Service, December 11, 2001. http://fpc.state.gov/ documents/organization/7951.pdf.

Elsea Jennifer K., and R. Chuck Mason. *The Use of Federal Troops for Disaster Assistance: Legal Issues* (CRS Report No. RS22266). Washington DC: Congressional Research Service, November 28, 2008. https://www.fas.org/sgp/crs/natsec/RS22266.pdf.

E.W. "Should Twitter Block Islamic Snuff Videos?" *Economist*, Aug 21, 2014. http://www.economist.com/blogs/democracyinamerica/2014/08/twitter-terror-and-free-speech.

Feinman, Jay M. *Law 101: Everything You Need to Know About American Law*, 3rd edition. New York: Oxford University Press, 2010.

Felker, John. *Driving Mission Execution*. Washington DC: United States Coast Guard, February, 2011. http://www.dtic.mil/ndia/2011jointmissions/WednesdayFelker.pdf.

Finnegan, Lizzy. "CISA and The War on Privacy." *Breitbart*, November 10, 2015. http://www.breitbart.com/tech/2015/11/10/cisa-and-the-war-on-privacy.

Fischer, Robert J., Edward Halibozek, and Gion Green. *Introduction to Security*, 8th edition. Boston, MA: Butterworth-Heinemann, 2008.

Friedman, Thomas L. *The World is Flat 3.0: A Brief History of the 21st Century*. New York: Picador, 2007.

Fund for Peace. "Indicators." Accessed September 25, 2015. http://fsi.fundforpeace.org/indicators.

Gallagher, Mark A., and Michael Horta. "Cyber Joint Munitions Effectiveness Manual (JMEM)." *M&S Journal* (Summer 2013): 5–14.

Garner, Bryan A., ed. *Black's Law Dictionary*. 9th edition. St. Paul, MN: West Group, 2009.

Gaziano, Todd F. "The Use and Abuse of Executive Orders and Other Presidential Directives" *Texas Review of Law & Politics* 5, no. 2 (Spring 2001): 267–97.

Gibson, Christine. "Our 10 Greatest Natural Disasters." *American Heritage* 57, no. 4 (August/September 2006). http://www.americanheritage.com/content/our-10-greatest-natural-disasters.

Gierow, Hauke Johannes. "Cyber Security in China: New Political Leadership Focuses on Boosting National Security." *China Monitor of the Mercator Institute for China Studies* 20 (December, 9 2014).

Giles, Keir. "Russia's Public Stance on Cyberspace Issues." In *Proceedings of 2012 International Conference on Cyber Conflict*, edited by Christian Czosseck, Rain Ottis, and Katharina Ziolkowski. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, June 5–8, 2012. https://ccdcoe.org/publications/2012proceedings/CyCon_2012_Proceedings.pdf.

Glennon, Michael J. *The Fog of Law*. Washington D.C.: Woodrow Wilson Center Press, 2010.

———. "The Road Ahead: Gaps, Leaks and Drips." *International Law Studies* 89 (2013): 362–86.

Gnambs, Timo. "What Makes a Computer Wiz? Linking Personality Traits and Programming Aptitude." *Journal of Research in Personality* 58 (October 2015): 31–34.

Goitein, Elizabeth, and David M. Shapiro, “Reducing Overclassification Through Accountability.” New York University School of Law. New York: New York University, October 5, 2011. http://www.brennancenter.org/sites/default/files/legacy/Justice/LNS/ Brennan_Overclassification_Final.pdf

Goodman, Will. “Cyber Deterrence: Tougher in Theory than in Practice.” *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 102–135.

Granick, Jennifer. “OmniCISA Pits DHS Against the FCC and FTC on User Privacy.” *Just Security*, December 16, 2015, https://www.justsecurity.org/28386/omnicisa-pits-government-against-self-privacy.

Gray, Chris Hables. *Cyborg Citizen: Politics in the Posthuman Age*. New York: Routledge, 2002.

Greenburg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. *Information Warfare and International Law*. Washington DC: Department of Defense, 1997.

Greenemeier, Larry. “A Quick Guide to the Senate's Newly Passed Cybersecurity Bill: The Basics of the Controversial Cybersecurity Information Sharing Act (CISA).” *Scientific American*, October 28, 2015. http://www.scientificamerican.com/article/a-quick-guide-to-the-senate-s-newly-passed-cybersecurity-bill.

Gutierrez, Carlos Jose. “Conflicts Between Domestic and International Law.” *The American University Law Review* 30, no. 1 (Fall 1980): 147–154.

Halperin, Morton H., Priscilla Clapp, and Arnold Kanter. “Organizational Interests.” In *Bureaucratic Politics and Foreign Policy,* 2nd edition. Washington D.C.: The Brookings Institution, 2006.

Hames, Joanne Banker, and Yvonne Ekern. *Introduction to Law*, 2nd edition. Upper Saddle River, NJ: Prentice Hall, 2002.

Hammond, Matthew Carlton. “The Posse Comitatus Act: A Principle in Need of Renewal.” *Washington University Law Quarterly* 75, no. 2 (1997): 953–84. http://openscholarship.wustl.edu/law_lawreview/vol75/iss2/11.

Hart, Catherine, Dal Yong Jin, and Andrew Feenberg. “The Insecurity of Innovation: A Critical Analysis of Cybersecurity in the United States.” *International Journal of Communication* 8 (2014): 2860–78. http://ijoc.org/index.php/ijoc/article/viewFile/2774/1257.

Hart, Gary, and Warren B. Rudman. *Road Map for National Security: Imperative for Change*. Report submitted by the U.S. Commission on National Security/21st Century. Phase III. (Washington DC: Government Publishing Office, February 15, 2001). http://govinfo.library.unt.edu/nssg/PhaseIIIFR.pdf.

Hartman, John Dale. *Legal Guidelines for Covert Surveillance Operations in the Private Sector*. Boston, MA: Butterworth-Heinemann, 1993.

Hayden, Michael, Jeffrey Eisenach, and Mike Daniels. "America's Strategy for Cyberspace: Is it Working?" Lecture. American Enterprise Institute Global Internet Strategy event, Washington DC, October 27, 2015. https://www.aei.org/wp-content/uploads/2015/10/Transcript1.pdf.

Hennessey, Susan. "The Problems CISA Solves: ECPA Reform in Disguise." *Lawfare*, December 23, 2015. https://www.lawfareblog.com/problems-cisa-solves-ecpa-reform-disguise.

———. "CISA in Context: Government Use and What Really Matters for Civil Liberties." Lawfare, January 14, 2016. https://www.lawfareblog.com/ cisa-context-government-use-and-what-really-matters-civil-liberties.

Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security: Strategic Security in the Cyber Age* 4, no. 2 (Summer 2011). doi: 10.5038/1944-0472.4.2.1.

Hlad, Jennifer. "Just Do It." *Air Force Magazine*, March 10, 2016. http://www.airforcemag.com/DRArchive/Pages/2016/March%202016/March%2010%202016/Just-Do-It.aspx.

Hoffman, Bruce, Edwin Meese III, and Timothy J. Roemer. "The FBI: Protecting the Homeland in the 21st Century." Report of the Congressionally-directed *9/11 Review Commission* to the Director of the Federal Bureau of Investigation. Washington DC: Government Publishing Office, March, 2015. https://www.fbi.gov/ stats-services/publications/protecting-the-homeland-in-the-21st-century.

Hoffmeister, Thaddeus. "An Insurrection Act for the 21st Century." Draft paper from the *Selected Works of Thaddeus Hoffmeister*. Dayton, OH: University of Dayton, 2009. http://works.bepress.com/thaddeus_hoffmeister/6.

Hollis, Duncan B. "Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?" In *Cyber War: Law and Ethics for Virtual Conflicts*, edited by Jens David Ohlin, Claire Finkelstein, and Kevin Govern. Oxford: Oxford University Press, 2015.

Howell, Elizabeth. “The Ocean Is A Lot Like Outer Space.” Universe Today: *Space and Astronomy News*, January 23, 2013. http://www.universetoday.com/99593/the-ocean-is-a-lot-like-outer-space.

Human Rights Watch. “USA and Torture: A History of Hypocrisy.” *www.hrw.org*, December 9, 2014. Accessed March 11, 2016. https://www.hrw.org/news/2014/12/09/usa-and-torture-history-hypocrisy.

Internet Live Stats. “Internet Users.” Accessed January 20, 2016. http://www.internetlivestats.com/internet-users.

Jaycox, Mark. “Broad Coalition of Groups Oppose CFAA Amendment to CISA Surveillance Bill.” *Electronic Frontier Foundation*, October 3, 2015. https://www.eff.org/deeplinks/2015/10/bipartisan-groups-oppose-cfaa-amendment-cisa-surveillance-bill.

Jordan, Tim. *Cyberpower: The Culture and Politics of Cyberspace and the Internet*. New York: Rutledge, 1999.

Kaldor, Mary. *New and Old Wars: Organized Violence in a Global Era*, 3rd edition. Stanford, CA: Stanford University Press, 2012.

Kamis, Ben, and Thorsten Thiel. “The Original Battle Trolls: How States Represent the Internet as a Violent Place.” Working paper for *ECPR General Conference*. Bordeaux, France: ECPR, September 5–7, 2013). http://ecpr.eu/filestore/paperproposal/25127ed8-317f-4039-8239-b2d06e456573.pdf.

Kean, Thomas H., and Lee Hamilton. *Executive Summary of The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. National Commission on Terrorist Attacks upon the United States (Washington DC: Government Publishing Office 2004).

Kean, Thomas H., and Lee Hamilton, *et al. The 9/11 Commission Report*. National Commission on Terrorist Attacks Upon the United States (Washington DC: Government Publishing Office, 2004).

Kelly, Brian B. "Investing in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' Can and Should Influence Cybersecurity Reform,” *Boston University Law Review* 92, no. 5 (March 2012): 1663–1711. http://www.bu.edu/law/journals-archive/bulr/volume92n4/documents/kelly.pdf.

Kerr, Orin S. “Vagueness Challenges to the Computer Fraud and Abuse Act.” *Minnesota Law Review* 94, vol. 1561 (2010). http://minnesotalawreview.org/wp-content/uploads/2012/03/Kerr_MLR.pdf.

Klotter, John C., and Jacqueline R. Kanovitz. *Constitutional Law: Justice Administration Legal Series*, 6th edition. Cincinnati, OH: Anderson, 1991.

Kugler, Richard L. "Deterrence of Cyber Attacks." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry Wentz. Dulles, VA: National Defense University Press, 2009.

La Bash, Miranda, and Christopher Landis. "Legal, Policy, and Organizational Impediments to the Protection of Critical Infrastructure from Cyber Threats." Master's thesis, Carnegie Mellon University, 2013.

Larson, Eric V., and John E. Peters. "Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options." Monograph report, Rand Corporation, 2001. http://www.rand.org/pubs/monograph_reports/MR1251.html.

Lawson, Sean. "Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States," *First Monday* 17, no. 7 (July, 2012). http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270.

Lieberthal, Kenneth. "The U.S. Intelligence Community and Foreign Policy: Getting Analysis Right." *The John L. Thornton China Center at The Brookings Institute*. Washington DC: Brookings Institute, 2009. http://www.brookings.edu/~/media/research/files/papers/2009/9/intelligence-community-lieberthal/09_intelligence_community_lieberthal.pdf.

Lindsay, Jon R. "Tipping the Scales: The Attribution Problem and The Feasibility of Deterrence Against Cyberattack." *Journal of Cybersecurity* (2015): 1–15. doi: 10.1093/cybsec/tyv003.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*, 5th edition. Washington DC: SAGE, 2012.

Macdonald, Stuart, and David Mair. "Terrorism Online: A New Strategic Environment." In *Terrorism Online: Politics, Law and Technology*, edited by Lee Jarvis, Stuart Macdonald, and Thomas M. Chen. New York: Routledge, 2015.

Malor, Gabriel. "Cut the Crap, Apple, and Open Syed Farook's iPhone." *The Federalist*, February 19, 2016. http://thefederalist.com/2016/02/19/cut-the-crap-apple-and-open-syed-farooks-iphone.

Matherly, John. Twitter post. August 28, 2014, 10:49 a.m. https://twitter.com/achillean.

May, Peter J. Ashley E. Jochim, and Joshua Sapotichne, “Constructing Homeland Security: An Anemic Policy Regime.” *Policy Studies Journal* 39, no. 2 (May 2, 2011): 285–307. doi: 10.1111/j.1541-0072.2011.00408.x.

Mendel, William W. “Combat in Cities: The LA Riots and Operation Rio.” Fort Leavenworth, KS: Foreign Military Studies Office, July, 1996. http://fmso.leavenworth.army.mil/documents/rio.htm.

Miller, Greg. “Muslim Cleric Aulaqi Is 1st U.S. Citizen on List of Those CIA Is Allowed To Kill.” *Washington Post*, April 7, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/04/06/AR2010040604121.html.

Moagoto, Jackson Nyamuya. *Battling Terrorism: Legal Perspectives on the Use of Force and the War on Terror*. New York: Routledge, 2005.

Morgan, Patrick M. “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm.” In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington D.C.: The National Academies Press, 2010.

Moyo, Dambisa, and Niall Ferguson. *Dead Aid: Why Aid Is Not Working and How There Is a Better Way for Africa*. New York: Farrar, Straus and Giroux, 2009.

Mulford, Laurie A. “Let Slip the Dogs of (Cyber) War: Progressing Towards a Warfighting U.S. Cyber Command.” Master’s thesis, National Defense University, Joint Forces Staff College, 2013.

Nakashima, Ellen. “Chinese Hack of Federal Personnel Files Included Security-Clearance Database.” *Washington Post*, June 12, 2015. https://www.washingtonpost.com/world/national-security/chinese-hack-of-government-network-compromises-security-clearance-files/2015/06/12/9f91f146-1135-11e5-9726-49d6fa26a8c6_story.html.

———. “NSA’s Bulk Collection of Americans’ Phone Records Ends Sunday.” *Washington Post*, November 27, 2015, https://www.washingtonpost.com/world/national-security/nsas-bulk-collection-of-americans-phone-records-ends-sunday/2015/11/27/ 75dc62e2-9546-11e5-a2d6-f57908580b1f_story.html.

Nelson, Catherine B., Jeannie A. Stamberger, and Brian D. Steckler. “The Evolution of Hastily Formed Networks for Disaster Response: Technologies, Case Studies, and Future Trends.” Conference Paper, IEEE Global Humanitarian Technology Conference, 2011. http://www.cisco.com/c/dam/en_us/about/doing_business/business_continuity/Paper_124_MSW_USltr_format.pdf.

North Atlantic Treaty Organization. “A Short History of NATO.” Accessed December 10, 2015. http://www.nato.int/history/nato-history.html.

———. Cooperative Cyber Defence Center of Excellence. “Research.” Accessed January 17, 2016. https://ccdcoe.org/research.html.

O’Leary, David P. “Beyond Measure: New Approaches to Analyzing Congressional Oversight of Homeland Security.” Master’s thesis, Naval Postgraduate School, 2015.

Obama, Barack. Interview by Candy Crowley. *CNN*, December 21, 2014. http://cnnpressroom.blogs.cnn.com/2014/12/21/cnns-candy-crowley-interviews-president-barack-obama.

Olsen, Kathleen K. “Cyberspace as Place and the Limits of Metaphor,” *Convergence: The Journal of Research into New Media Technologies* 11, no. 1 (Spring 2005): 10–18, http://www.andredeak.com.br/pdf/cyberspace.pdf.

Orentilicher, Diane F. “Unilateral Multilateralism: United States Policy Toward the International Criminal Court.” *Cornell International Law Journal* 36, no. 3 (2004): 415–33. http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1526&context=cilj.

Panetta, Leon. Interview by Jim Lehrer. *PBS New Hour*, May 3, 2011. http://www.pbs.org/newshour/bb/terrorism-jan-june11-panetta_05-03.

———. “Remarks on Cybersecurity.” Speech, Business Executives for National Security. New York, October 11, 2012. Published in *Council on Foreign Relations*, October 12, 2012. http://www.cfr.org/cybersecurity/ secretary-panettas-speech-cybersecurity/p29262.

Penn, Megan. “Organized Cyber Crime: Comparison of Criminal Groups in Cyberspace.” *Cyber Defense Review,* April 7, 2015. http://www.cyberdefensereview.org/2015/04/07/organized-cyber-crime.

Peterson, Andrea. “The NSA Has Its Own Team of Elite Hackers,” *Washington Post*, August 29, 2013. https://www.washingtonpost.com/ news/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers.

Pew Research. “Cyber Attacks Likely to Increase.” October 29, 2014 http://www.pewinternet.org/files/2014/10/PI_FutureofCyberattacks_102914_pdf.pdf.

Pfanner, Toni. “Military Uniforms and the Rule of Law.” *International Review of the Red Cross* 86, no. 853 (March 2004): 93–124.

Pomerleau, Mark. “In Cyber Defense, Can Cold War-Style Deterrence Work?” *Defense Systems*, April 20, 2015. https://defensesystems.com/articles/2015/04/20/dod-cyber-deterrence.aspx

Radziwill, Yaroslav. *Cyber-Attacks and the Exploitable Imperfections of International Law*. Leiden, The Netherlands: Koninklijke Brill, 2015.

Ramsay, James D., and Linda Kiltz, eds. *Critical Issues in Homeland Security: A Casebook*. Boulder, CO: Westview Press, 2014.

Rauscher, Karl. “It’s Time to Write the Rules of Cyberwar: The World Needs a Geneva Convention for Cybercombat.” *IEEE Spectrum*, November 27, 2013. http://spectrum.ieee.org/telecom/security/its-time-to-write-the-rules-of-cyberwar.

Rollins, John, and Anna C. Henning. *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations* (CRS Report No. R4042). Washington DC: Congressional Research Service, March 10, 2009. http://www.fas.org/sgp/crs/natsec/R40427.pdf.

Romeo, Jim. “The Hacker Beside You.” *Transaction World Magazine*, May 1, 2014. www.transactionworld.net/articles/2014/may/cover-story.html.

Rosegrant, Susan. “The Flawed Emergency Response to the 1992 Los Angeles Riots.” Case study in *Executive Session on Domestic Preparedness, John F. Kennedy School of Government*. Report no. C16-00-1586.0. Cambridge, MA: Harvard University, 2000. http://www.ksg.harvard.edu/research/publications/cases/1586_0.pdf.

Rosenzweig, Paul. “The Cybersecurity Act of 2015.” *Lawfare*, December 16, 2015. https://www.lawfareblog.com/cybersecurity-act-2015.

Roser, Max. “Democratisation.” Our World in Data. Accessed November 4, 2015. http://ourworldindata.org/data/political-regimes/democratisation.

Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 1966.

Schmalleger, Frank J. *Criminal Justice: A Brief Introduction*, 9th edition. Upper Saddle River, NJ: Prentice Hall, 2012.

Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press, 2013.

Schneier, Bruce. “The Public-Private Surveillance Partnership.” *Bloomberg Businessweek*, July 31, 2013. http://www.bloombergview.com/articles/2013-07-31/the-public-private-surveillance-partnership.

Sen, Tapan. “Congressional Oversight of Homeland Security: Help or Hindrance?” Master’s thesis, Naval Postgraduate School, 2012.

Sharp, Walter Gary, Sr. *CyberSpace and the Use of Force*. Falls Church, VA: Aegis Research Corporation, 1999.

Simmons, Noah. “A Brave New World: Applying International Law of War to Cyber-Attacks.” Journal of Law & Cyber Warfare 4, no. 1 (Winter 2014): 42–108.

Solis, Gary D. “Cyber Warfare.” *Military Law Review* 219 (Spring 2014): 1–52. http://www.loc.gov/rr/frd/Military_Law/Military_Law_Review/pdf-files/219-spring-2014.pdf.

Soucy, Jon. “Guard Set To Activate Additional Cyber Units.” *National Guard Bureau*, December 9, 2015. http://www.nationalguard.mil/News/ArticleView/tabid/5563/Article/633547/guard-set-to-activate-additional-cyber-units.aspx.

Snowden, Edward. “Open Letter to the Brazilian People,” *Folha de S Paulo*, December 17, 2013. Reprinted in *The Guardian*, December 17, 2013. http://www.theguardian.com/world/2013/dec/17/edward-snowden-letter-brazilian-people.

Stahel, W. R. “The Service Economy: ‘Wealth Without Resource Consumption’?” *Philosophical Transactions: Mathematical, Physical and Engineering Sciences* 355, no. 1728 (July, 1997): 1309–1320 http://www.jstor.org/stable/54751.

Stavridis, James, and David Weinstein. “Time for a US Cyber Force.” *Proceedings* 140, no. 1 (January 2014): 40–44.

Steger, Manfred B. *Globalization: A Very Short Introduction*. Oxford: Oxford University Press, 2013.

Sterling, Christopher H. Phyllis W. Bernt, and Martin B.H. Weiss *Shaping American Telecommunications: A History of Technology, Policy, and Economics*. New York: Routledge, 2005.

Sternstein, Aliya. “$460M CYBERCOM Contract Will Create Digital Munitions.” *Defense One*, October 5, 2015. http://www.defenseone.com/technology/2015/10/460m-cybercom-contract-will-create-digital-munitions/122556.

Sturgis, Emma. “10 Myths About Hackers (That Are Totally False).” *Nerd Like You*, September 8, 2015, http://www.nerdlikeyou.com/10-myths-about-hackers-that-are-totally-false.

Task Force on Streamlining and Consolidating Congressional Oversight of the U.S. Department of Homeland Security. *Streamlining and Consolidating Congressional Oversight of the U.S. Department of Homeland Security*. Washington DC: Aspen Institute, September 2013. http://www.aspeninstitute.org/sites/default/files/content/docs/pubs/Sunnylands%20report%2009-11-13.pdf.

Tatem, Andrew J., Simon I. Hay, and David J. Rogers. "Global Traffic and Disease Vector Dispersal." *Proceedings of the National Academy of Sciences of the United States of America* 103, no. 16 (April 18, 2006): 6242–47. doi:10.1073/pnas.0508391103.

Taylor, Guy. "CIA Goes Live with New Cyber Directorate, Massive Internal Reorganization." *Washington Times*, October 1, 2015. http://www.washingtontimes.com/news/2015/oct/1/cia-goes-live-with-new-cyber-directorate-massive-i.

Tekie, Isaac. "Bringing the Troops Home to a Disaster: Law, Order, and Humanitarian Relief." *Ohio State Law Journal* 67, no. 5 (2006): 1227–64. http://hdl.handle.net/1811/71058.

Timm, Trevor. "Wall Street Journal Columnist Repeatedly Gets His Facts Wrong About NSA Surveillance." *Electronic Frontier Foundation*, November 27, 2013. https://www.eff.org/deeplinks/2013/11/wall-street-journal-columnist-gordon-crovitz-repeatedly-gets-his-facts-wrong-about.

Tollestrup, Jessica. *The Congressional Appropriations Process: An Introduction* (CRS Report No. R42388). Washington DC: Congressional Research Service, November 14, 2014. http://www.senate.gov/CRSReports/crs-publish.cfm?pid=%260BL%2BP%3C%3B3%0A.

Trujillo, Clorinda. "The Limits of Cyberspace Deterrence," *Joint Force Quarterly* 75 (4th Qtr. 2014): 43–52.

United Nations. *Charter of The United Nations*. October 24, 1945. Ch. I, Art. 1. Accessed December 10, 2015. http://www.un.org/en/sections/un-charter/chapter-i/index.html.

———. "History of the United Nations." Accessed December 10, 2015. http://www.un.org/en/sections/history/history-united-nations.

———. General Assembly. *Developments in the Field of Information and Telecommunications in the Context of International Security Resolution*. June 26, 2015. A/70/172. Accessed March 9, 2016. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/172.

———. General Assembly. *International Bill of Human Rights.* December 10, 1948. A/RES/217(III). Accessed November 8, 2015. http://www.undocs.org/A/RES/217(III).

United States Army. International and Operational Law Department. "Operational Law Handbook." Edited by David H. Lee. The Judge Advocate General's Legal Center and School, 2015. https://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdf.

United States Central Intelligence Agency. "Offices of CIA: Digital Innovation." Last modified October 1, 2015. https://www.cia.gov/offices-of-cia/digital-innovation/index.html.

———. Office of the Chief Information Officer's Information Management Services. "Bay of Pigs Release" Last modified August 2, 2011. http://www.foia.cia.gov/collection/bay-pigs-release.

———. Office of the Director of the Central Intelligence Agency. *CIA Comments on the Senate Select Committee on Intelligence Report on the Rendition, Detention, and Interrogation Program*. Washington DC: CIA, June 27, 2013. https://www.cia.gov/library/reports/CIAs_June2013_Response_to_the_SSCI_Study_on_the_Former_Detention_and_Interrogation_Program.pdf. Document was sanitized and declassified on December 8, 2014.

United States Coast Guard. Office of the Commandant of the United States Coast Guard. *United States Coast Guard Cyber Strategy*. Washington DC: Department of Homeland Security, June, 2015. https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf.

United States Congress. House of Representatives. *Conference Report On the Intelligence Authorization Act for Fiscal Year 1991*. 102nd Cong., 1st sess., July 25, 1991. H. Rep. 102-166. http://www.intelligence.senate.gov/sites/default/files/publications/102166.pdf.

———. House of Representatives. "Lofgren, Wyden, Paul Introduce Bipartisan, Bicameral Aaron's Law to Reform Computer Fraud and Abuse Act." Press release by Peter Whippy, April 21, 2015. Accessed August 11, 2015, https://lofgren.house.gov/news/documentsingle.aspx?DocumentID=397911.

———. House of Representatives. Committee On Foreign Affairs. *Cyber Attacks: An Unprecedented Threat to U.S. National Security: Hearing Before the Subcommittee On Europe, Eurasia, And Emerging Threats of the Committee On Foreign Affairs*. 113th Cong., 1st sess., March 21, 2013, No. 113-8. http://docs.house.gov/meetings/FA/FA14/ 20130321/100547/HHRG-113-FA14-20130321-SD002.pdf.

———. House of Representatives. Committees on Oversight and Government Reform, Homeland Security, Select Intelligence (Permanent Select), Armed Services, the Judiciary, Foreign Affairs, Science, Space, and Technology, and Energy and Commerce. *A Bill to Repeal the Cybersecurity Act of 2015*. 114th Cong., 2nd sess., January 8, 2016. H.R. 4350. https://www.congress.gov/114/bills/hr4350/ BILLS-114hr4350ih.pdf.

———. House of Representatives. Committee on Rules. *Rules of the House of Representatives of the United States One Hundred Thirteenth Congress*. 113th Cong., 2nd sess., May 21, 2015. H. Doc. 113-181. https://www.gpo.gov/fdsys/pkg/HMAN-114/pdf/HMAN-114.pdf.

———. House of Representatives. Permanent Select Committee on Intelligence. *Report to Accompany H.R. 2701, 'The Intelligence Authorization Act for Fiscal Year 2010.'* 111th Cong., 1st sess., June 26, 2009. H. Rep. 111-186. https://www.congress.gov/111/crpt/hrpt186/CRPT-111hrpt186.pdf.

———. Senate. Committee on Rules and Administration. *Standing Rules of the Senate*. 113th Cong., 1st sess., January 24, 2013. S. Doc. 113-18. https://www.gpo.gov/fdsys/pkg/CDOC-113sdoc18/pdf/CDOC-113sdoc18.pdf.

———. Senate. Committee On The Judiciary. *The War Against Terrorism: Working Together to Protect America*. 108th Cong., 1st sess., March 4, 2013. https://www.judiciary.senate.gov/imo/media/doc/mueller_testimony_03_04_03.pdf.

———. Senate. Select Committee on Intelligence. *Committee Study of the Central Intelligence Agency's Detention and Interrogation Program*. 113th Cong., 2nd sess., December 9, 2014. S. Rep. 113-288. http://www.intelligence.senate.gov/sites/default/files/documents/CRPT-113srpt288.pdf. Document was sanitized and declassified on December 3, 2014.

———. Senate. Select Committee on Intelligence. *FISA Improvements Act of 2013*. 113th Cong., 1st sess., 2013. S. 1631. https://www.congress.gov/113/bills/s1631/BILLS-113s1631pcs.pdf.

United States Department of Commerce. United States Census Bureau. "Profile America Facts for Features: Hurricane Katrina 10th Anniversary." No. CB15-FF.16. Washington DC: Department of Commerce, Aug. 29, 2015. https://www.census.gov/newsroom/facts-for-features/2015/cb15-ff16.html.

United States Department of Defense. *The Department of Defense Cyber Strategy*. Washington DC: Department of Defense, April, 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

———. Air Land Sea Application Center. *Multi-Service Tactics, Techniques, And Procedures for Defense Support of Civil Authorities (DSCA) (ATP 3-28.1/MCWP 3-36.2/NTTP 3-57.2/AFTTP 3-2.67)*. Joint Base Langley-Eustis, VA: Air Land Sea Application Center, September, 2015. http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/atp3_28x1.pdf.

———. Center for Army Lessons Learned. *Catastrophic Disaster Response Staff Officer's Handbook*. No. 06-8. Fort Leavenworth, KS: Combined Arms Center, May, 2006). http://usacac.army.mil/sites/default/files/publications/06-08.pdf.

———. National Security Agency. *Cryptologic Almanac 50th Anniversary Series: The Central Security Service*. Washington DC: Department of Defense, 2002. https://www.nsa.gov/public_info/_files/crypto_almanac_50th/The_CSS.pdf. DOCID: 3575724 is now declassified.

———. Office of General Council. "Law of War Manual." Washington DC: Department of Defense, June, 2015. http://www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June-2015.pdf.

———. Office of the National Security Agency Director of Civil Liberties and Privacy. *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*. Washington DC: Department of Defense, 2014. http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

———. United States Northern Command. "About USNORTHCOM." Accessed March 11, 2016 http://www.northcom.mil/ AboutUSNORTHCOM.aspx.

United States Department of Homeland Security. "Information Sharing." Last modified August 26, 2015. http://www.dhs.gov/topic/information-sharing.

———. "N-Kick," Last modified October 30, 2009. http://www.dhs.gov/blog/2009/10/30/n-kick.

———. "National Cybersecurity and Communications Integration Center" Accessed March 10, 2016. https://www.us-cert.gov/nccic.

———. Federal Emergency Management Agency. "FEMA Regional Offices." Accessed March 10, 2016. https://emilms.fema.gov/IS800B/lesson4/NRF0104190t.htm.

———. Federal Emergency Management Agency, *National Response Framework*. 2nd edition. Washington DC: Department of Homeland Security, 2013. https://www.fema.gov/ media-library-data/20130726-1914-25045-1246/final_national_response__framework_20130501.pdf.

———. Federal Emergency Management Agency. “National Response Framework: Stafford Act Support to States.” Accessed March 10, 2016. https://www.fema.gov/pdf/emergency/nrf/nrf-stafford.pdf.

———. National Cybersecurity and Communications Integration Center. “Incident Response Activity.” *ICS-CERT* Monitor (September 2014–February 2015): 1–5. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ ICS-CERT_Monitor_Sep2014-Feb2015.pdf.

———. National Cybersecurity and Communications Integration Center. “Coordinated Vulnerability Disclosures.” *ICS-CERT* Monitor (September 2014–February 2015): 12–14. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.

———. National Cybersecurity and Communications Integration Center. “Fact Sheet: Industrial Control Systems Cyber Emergency Response Team.” Accessed March 10, 2016. https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_ICS-CERT_S508C.pdf.

———. National Protection and Programs Directorate. *Privacy Impact Assessment Update for the Private Sector Clearance Program for Critical Infrastructure, PIA-020(a)*. Washington DC: Department of Homeland Security, 2015. https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-pscp-february2015.pdf.

———. Office of Infrastructure Protection. *2015 Commercial Facilities Sector-Specific Plan*. Washington DC: Department of Homeland Security, 2015. https://www.dhs.gov/ sites/default/files/publications/nipp-ssp-commercial-facilities-2015-508.pdf.

———. Office of Infrastructure Protection. *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*. Washington DC: Department of Homeland Security, 2010. http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf.

———. Office of Inspections and Special Reviews, *A Performance Review of FEMA’s Disaster Management Activities in Response to Hurricane Katrina*. Report no. OIG-06-32. Washington DC: Department of Homeland Security, March 2006. https://www.oig.dhs.gov/assets/Mgmt/OIG_06-32_Mar06.pdf.

———. Office of the Secretary of Homeland Security. *National Response Plan, 2004*. Washington DC: Department of Homeland Security, December 2004. https://it.ojp.gov/fusioncenterguidelines/NRPbaseplan.pdf.

———. United States Computer Emergency Readiness Team. “National Cybersecurity and Communications Integration Center.” Accessed March 10, 2016. https://www.us-cert.gov/nccic.

———. United States Secret Service. “CYBER CRIME: The U.S. Secret Service Partners with State, Local and International Law Enforcement to Pursue the World’s Most Wanted Cyber Criminals.” Trifold handout at Massachusetts Collectors and Treasurers Association Virtual Conference, June 14–17, 2015. Washington DC: Department of Homeland Security, March 3, 2015. http://mcta.virtualtownhall.net/pages/MCTA_Presentations/2015-06/USSS%20Cyber%20Programs%20phamphlet%203-13-15.pdf.

United States Department of Justice. Federal Bureau of Investigation. “Cyber’s Most Wanted.” Accessed February 12, 2016. https://www.fbi.gov/wanted/cyber.

———. Federal Bureau of Investigation. “The FBI: A Centennial History, 1908–2008.” Washington DC: Government Publishing Office, 2008. https://www.fbi.gov/about-us/history/a-centennial-history/the-fbi-a-centennial-history-1908-2008.

———. Federal Bureau of Investigation. Internet Crime Complaint Center. *2014 Internet Crime Report*. Washington DC: Department of Justice, May 10, 2014. https://www.fbi.gov/news/news_blog/2014-ic3-annual-report.

———. Federal Bureau of Investigation. National Cyber Investigative Task Force. “Addressing Threats to the Nation’s Cybersecurity.” Accessed January 12, 2016. https://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity-1.

———. Bureau of Justice Assistance. “Cybersecurity in Congressional Research Service Reports.” Accessed March 10, 2016. https://it.ojp.gov/PrivacyLiberty/reports/service/2336.

———. Bureau of Justice Assistance, Department of Homeland Security Office for Civil Rights and Civil Liberties, and Department of Homeland Security Privacy Office. “Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510–22.” Last modified July 30, 2013. https://it.ojp.gov/privacyliberty/authorities/statutes/1285.

———. Computer Crime and Intellectual Property Section. *Searching and Seizing Computers and Obtaining Electronic Evidence In Criminal Investigations*. Washington DC: Office of Legal Education, January 14, 2009. http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

———. Computer Crime and Intellectual Property Section. *Prosecuting Computer Crimes*. 2nd edition. Washington DC: Office of Legal Education, 2015. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

———. Office of Inspector General. *A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008*. Washington DC: Department of Justice, September 2012. https://oig.justice.gov/reports/2015/o1501.pdf. Document was sanitized and declassified on January 9, 2015.

———. Organized Crime and Racketeering Section. *Criminal RICO: 18 U.S.C. §§ 1961–1968, A Manual for Federal Prosecutors*. 5th edition. Washington DC: Department of Justice, October, 2009. http://www.justice.gov/sites/default/files/usam/legacy/2014/10/17/rico.pdf.

United States Department of Treasury. Federal Reserve Banks. *Fedwire Funds Service Disclosure*. Washington DC: WPO, December 24, 2015. https://www.frbservices.org/files/serviceofferings/pdf/fedwire-funds-service-disclosure.pdf.

United States Foreign Intelligence Surveillance Court. "In Re Production of Tangible Things [Redacted]." Docket No. BR 08-13 (FISC, March 2, 2009). http://www.dni.gov/files/documents/0328/039.%20A4000915%20%20BR%2008-13%20%20Order%20(3-2-09)%20Redacted%2020140327.pdf. Document was sanitized and declassified on March 28, 2014.

United States National Guard Association. "NGAUS Fact Sheet: Understanding the Guard's Duty Status." Accessed March 14, 2016. http://www.ngaus.org/sites/default/files/Guard%20Statues.pdf.

United States Office of the Chairman of the Joint Chiefs of Staff. *Cyberspace Operations*. Joint Publication 3-12 (R). Washington DC: Chairman Joint Chiefs of Staff, February 5, 2013.

———. *Doctrine for the Armed Forces of the United States*. Joint Publication 1-0. Washington DC: Chairman Joint Chiefs of Staff, March 25, 2013.

———. *Joint Operational Planning*. Joint Publication 5-0. Washington, DC: Chairman Joint Chiefs of Staff, August 11, 2011.

———. *Joint Operations*. Joint Publication 3-0. Washington DC: Chairman Joint Chiefs of Staff, August 11, 2011.

United States Office of the Director of National Intelligence. “IC on the Record.” Accessed March 9, 2016. http://icontherecord.tumblr.com/search/IG+report.

———. “Timeline.” Accessed January 10, 2016. http://www.nctc.gov/site/timeline.html.

———. “Statement by the ODNI and the U.S. DOJ on the Declassification of Documents Related to the Protect America Act Litigation.” Office of the Director of National Intelligence press release, September 11, 2014. Accessed January 8, 2016. http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1109-statement-by-the-office-of-the-director-of-national-intelligence-and-the-u-s-department-of-justice-on-the-declassification-of-documents-related-to-the-protect-america-act-litigation?tmpl=component&format=pdf.

———. National Counterterrorism Center. “Methods & Tactics.” Accessed January 10, 2016. http://www.nctc.gov/site/methods.html#sarin.

United States White House. *The National Strategy to Secure Cyberspace*. Washington DC: White House, February, 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

———. *The National Security Strategy of the United States, 2002*. Washington, DC: White House, February, 2002.

———. *The National Security Strategy of the United States, 2015*. Washington, DC: White House, February, 2015.

———. *The National Strategy for Information Sharing and Safeguarding*. Washington DC: White House, December, 2012.

———. *Presidential Policy Directive for Critical Infrastructure Security and Resilience/PPD-21*. Washington DC: White House, February 12, 2013.

———. “National Security Council.” Accessed March 11, 2016. https://www.whitehouse.gov/administration/eop/nsc.

———. Office of the Press Secretary. “Remarks by the President in a Press Conference.” United States Office of the Press Secretary press release, August 9, 2013. Accessed March 9, 2016. https://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.

———. Office of the Press Secretary. “SECURING CYBERSPACE – President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts.” United States Office of the Press Secretary press release, January 13, 2015. Accessed March 11, 2015. https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

Van Wagenen, James S. “A Review of Congressional Oversight: Critics and Defenders.” *CIA Center for the Study of Intelligence*, April 14, 2007. Last modified June 27, 2008. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/wagenen.html.

VanDriel, Martha S. H. “Bridging the Planning Gap: Incorporating Cyberspace into Operational Planning.” *Strategic Studies Institute, United States Army War College*, May 4, 2015. http://www.strategicstudiesinstitute.army.mil/index.cfm/articles/Bridging-the-planning-gap/2015/05/04.

Varma, Corey. “What is the Computer Fraud and Abuse Act (CFAA)?” *Cyberspace Law, Information Technology And Privacy Law*, January 3, 2015. http://www.coreyvarma.com/2015/01/what-is-the-computer-fraud-and-abuse-act-cfaa/#protected_computer.

Ventre, Daniel, ed. *Cyber Conflict: Competing National Perspectives*. Hoboken, NJ: John Wiley & Sons, 2012.

Wall, Andru E. “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action.” *Harvard National Security Journal* 3, no. 1 (2012): 85–142. http://harvardnsj.org/wp-content/uploads/2012/01/Vol-3-Wall.pdf.

Walsh, Lawrence E. *Firewall: The Iran-Contra Conspiracy and Cover-Up*. New York: W.W. Norton, 1997.

Weimann, Gabriel. *Terror on the Internet: The New Arena, the New Challenges*. Washington DC: United States Institute of Peace Press, 2006.

Whitley, Joe D., and Lynne K Zusman, eds. *Homeland Security: Legal and Policy Issues*. Chicago: American Bar Association, 2009.

Williams, Brett. “Cyberspace: What Is It, Where Is It and Who Cares?” *Armed Forces Journal*, March 13, 2014. http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares.

Willis, Garry. *Bomb Power: The Modern Presidency and the National Security State*. New York: Penguin Books, 2010.

Wintgens, Luc, ed. *Legisprudence: New Theoretical Approach to Legislation*. Portland, OR: Hart, 2002.

Wyden, Ron. “Wyden Slams Latest, Worse Version of Cybersecurity Bill.” Ron Wyden press release, December 16, 2015. Accessed March 9, 2016. https://www.wyden.senate.gov/news/press-releases/wyden-slams-latest-worse-version-of-cybersecurity-bill.

Zenko, Micah. “Transferring CIA Drone Strikes to the Pentagon: Policy Innovation Memorandum No. 31.” Memorandum of the Council on Foreign Relations: Center for Preventative Action, April 16, 2013. http://i.cfr.org/content/publications/attachments/PIM_Drones_Zenko_Final_4_16_13.pdf.

Zetter, Kim. “NSA Hacker Chief Explains How to Keep Him Out of Your System.” *Wired*, January 28, 2016. http://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California